# Phoenix RSM

## User Guide

### Version 6.5

DCN: PhUser-05212015

SOLERATEC

# Table of Contents


## Introduction 5

**Software License Agreement** ... 7
**Contact Information** ... 10
**Documentation Overview** ... 11
**Hardware and Software Requirements** ... 12
**Product Licensing** ... 15
**Architectural Overview** ... 16
**Technical Overview** ... 18

## Installation 21

**Windows** ... 24
**Mac** ... 32
**Linux** ... 36

## Getting Started 38

**Quick Start** ... 40

## Vault Management 53

**Add Vaults** ... 54
**Add or Remove Vault Wizard** ... 56
**Disable SCSI Devices** ... 77
**Vault Admin** ... 80
**Vault Secure or Unsecure** ... 85
**Vault Shutdown or Restart** ... 86
**Vault Properties** ... 86
Vault Properties General Tab ... 87
Vault Properties Device Tab ... 89
Vault Properties Database Tab ... 93
Vault Properties License Tab ... 95
Vault Properties Security Tab ... 99
Vault Properties Logs Tab ... 103
Vault Properties Notifications Tab ... 104
Vault Properties Diagnostics Tab ... 107
**Vault Checkup** ... 109
**Prepare Media** ... 110
**Load Media** ... 120
**Reload Media** ... 123
**Unload Media** ... 124
**Erase Media** ... 128
**Start Vaults Manually** ... 129
**Vault Details** ... 129
**Network Activity** ... 135
**Mini Vault Stats** ... 138


© 2015

Vault Stats ... 140
Remove Vaults ... 145

## Camera Management 148

Add Camera Wizard ... 149
Camera Policies ... 158
Import/Export Recording Policies ... 162
Camera Policies Window ... 177
Camera Policies Camera Tab ... 181
Camera Policies Metadata Tab ... 186
Camera Policies Processing Tab ... 187
Camera Policies Destination Tab ... 189
Camera Policies Scheduling Tab ... 192
Camera Policies Advanced Tab ... 194
Camera Policies User Preferences ... 197
Camera Configurations ... 198
Camera Configurations Window ... 200
Import/Export Camera Configurations ... 203
Manually Add IP Camera ... 209
Add VMS Camera ... 218
Motion Detection ... 226

## Live Viewer 235

View Camera Feeds ... 239
View Camera Pool Feeds ... 239
Live Viewer Layout ... 240
Live Viewer Patrols ... 242
Camera Control: PTZ and Focus ... 244
Live Viewer User Preferences ... 247

## Surveillance Video Manager 251

SVM Search and Export ... 253
Search Surveillance Video ... 257
SVM Save and Load Export Queue ... 264
SVM Media Viewer and Logging ... 265
SVM Media Viewer ... 267
SVM Logging ... 272
Export Surveillance Video ... 277
SVM User Preferences ... 288

## Data Management 295

Data Service Policies ... 297
Import/Export Data Service Policies ... 300
Data Service Policies Window ... 311
Data Service Policies Source Tab ... 313

© 2015

Data Service Policies Criteria Tab ... 316
Data Service Policies Destination Tab ... 319
Data Service Policies Scheduling Tab ... 322
Data Service Policies Advanced Tab ... 326

Customization 331

Wildcards ... 332
Filters ... 343
ExportExtensions.cfg ... 349
MetadataExtensions.cfg ... 358
Site.cfg ... 368
Key Configurations ... 370

Command Line Arguments 398

Locator Admin Command Line ... 399
Locator Service ... 400
Vault Admin Command Line ... 401
Vault Service ... 405
Data Services Command Line ... 413
Data Services Service ... 423
Live Viewer Command Line ... 424

Job Scheduling 425

Troubleshooting 428

Manage Services 438

Glossary 441

Index 448

© 2015

# Introduction

We welcome you to SoleraTec's Phoenix RSM, version 6.5.

SoleraTec is in the business of data management and can effectively address storage needs for digital data assets.

With the SoleraTec solution, digital data assets are captured or ingested into the management solution's Information Repository, where they are stored under complete control, can be searched on, and retrieved with the highest original quality. Depending on the scope of your working environment, the Information Repository is made up of one Vault or many Vaults on your network; each Vault contains a central processing unit (CPU), Phoenix RSM software, and storage.

The Phoenix RSM solution is unique and outstanding compared to any storage management systems because of:

- **Decentralized Vaults** -Your Information Repository is distributed over your network. This offers you a dynamic, server-less solution with a "no single point of failure" where you can get to your data quickly and easily, at any time.
- **Scalable solution** - Rather than having one giant expensive storage unit, you can easily add storage space incrementally as your business grows and your data requirements increase. This promotes significant cost savings, as you can add less expensive storage units.
- **Multi-tiered storage** - Different types of storage units can be integrated into the solution at different times. This supports long-term retention needs and unlimited retention possibilities.
- **Online, near-line, and offline communication** - Low resolution companion or proxy files are created and completely managed by Phoenix RSM. These proxy files are stored locally but always teamed with high resolution originals, making it possible for thorough, worthwhile searches throughout your entire Information Repository. Phoenix RSM provides fast retrieval of original video or files, even if the media is stored offline.

## Phoenix RSM - A Video Surveillance Solution

Phoenix RSM is a live viewing and forensics-based software that provides complete surveillance video management. The Phoenix RSM video management system (VMS) seamlessly integrates all components from the camera, to any number of storage devices. Phoenix RSM includes extensive camera compatibility, as it can connect and configure to any RTSP-enabled IP camera, and it has an unlimited live video matrix, with the ability to view 16 channels at a time.

The Phoenix RSM solution manages unaltered high resolution original video and creates low resolution companion video (at a fraction of the original size), and then implements storage policies to replicate and migrate the video to and from a storage device, automatically, with no data loss.

Phoenix RSM manages a multi-tiered solution, meaning that it has a scalable architecture and can manage multiple storage devices. With the low resolution companion video, archives are active and available when video is located online, near-line, or offline. There is no cumbersome process of video backup and restoration that traditional single-tiered systems have.

© 2015

From capturing your video with Camera Policies, searching for and retrieving stored video using the Surveillance Video Manager and then reviewing using the Media Viewer, to viewing live video feeds with the Live Viewer, you will find that with Phoenix RSM all your video surveillance needs are met with ease.

See also Architectural Overview and Technical Overview.

## Seamless Integration

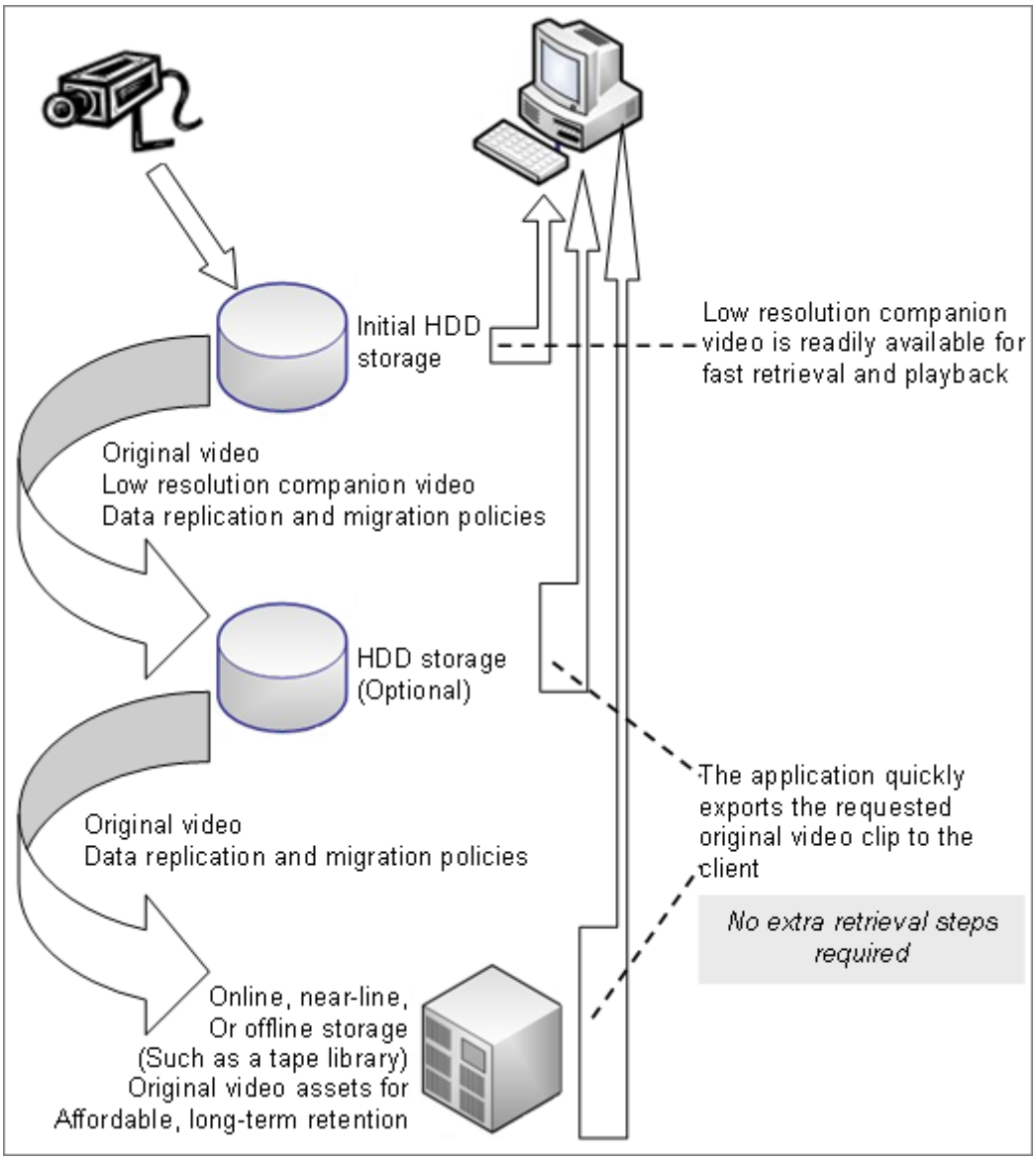
Seamless integration refers to the ease at which Phoenix RSM handles all your data asset management needs. From video capture, to online, near-line, or offline storage, to retrieving data for review or manipulation on your desktop client, all your data - regardless of when it was ingested, recorded or where stored - are under complete management and are easily accessible.

Phoenix RSM manages the unaltered high resolution original video and creates low resolution companion or proxy video (at a fraction of the original video size) along with customizable metadata to enable fast searches and video review. Phoenix RSM then implements storage policies to replicate and migrate the original, unaltered video between primary hard disk-based storage and other storage devices - such as data tape libraries, automatically, with no data loss and complete chain-of-custody. When searching for video, the low resolution companion video would be the primary video footage retrieved, but it is teamed with the original source video.

Phoenix RSM has a scalable, multi-tiered infrastructure, where it can manage multiple storage devices across a network for the most affordable long-term retention available.

The following is an example of a complete video lifecycle management solution. The illustrated data tape library can be substituted with any type of storage device.

© 2015


Initial HDD storage
Low resolution companion video is readily available for fast retrieval and playback
Original video
Low resolution companion video
Data replication and migration policies
HDD storage (Optional)
The application quickly exports the requested original video clip to the client
Original video
Data replication and migration policies
No extra retrieval steps required
Online, near-line, Or offline storage (Such as a tape library) Original video assets for Affordable, long-term retention

# Software License Agreement

The Software Programs/Utilities and documentation provided by SoleraTec under the name of Phoenix RSM are licensed only on the condition that you (referred to as “YOU” or “Licensee”) agree with SoleraTec (referred to as “Company”) to the terms and conditions set forth below.

**PLEASE READ THIS LICENSE AGREEMENT CAREFULLY BEFORE DOWNLOADING OR USING THE SOFTWARE OR DOCUMENTATION.**

**BY CLICKING ON THE "ACCEPT" BUTTON, OPENING THE PACKAGE, DOWNLOADING THE PRODUCT, OR USING THE EQUIPMENT THAT CONTAINS THIS PRODUCT, YOU ARE CONSENTING TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, CLICK THE "DO NOT ACCEPT" BUTTON AND THE INSTALLATION PROCESS WILL NOT CONTINUE, RETURN THE PRODUCT TO THE PLACE OF PURCHASE FOR A FULL REFUND, OR DO NOT DOWNLOAD THE PRODUCT.**

In consideration for use of the Software, Licensee hereby agrees to the following terms and conditions:

**1. DEFINITIONS**

**1.1** "Documentation" shall mean the documentation provided in connection with the Software.

**1.2** "Effective Date" shall mean the date on which Licensee opens the package, downloads the product, or uses equipment that contains the product.

**1.3** "Software" shall mean the object code of the Programs/Utilities included on the delivered digital media.

**2. TERMINATION**

**2.1** This Agreement may be terminated by Licensee at any time by destroying the Software, together with all copies thereof. This Agreement will also terminate automatically and without notice if Licensee fails to comply with any term or condition of this Agreement. Termination of this Agreement shall terminate Licensee's license to the Software. All other terms and conditions of this Agreement shall survive termination in perpetuity.

**3. LICENSE GRANT**

**3.1** Company grants to Licensee a nonexclusive, nontransferable license to use one (1) copy of the Software, in object code form only, on one computer, and the Documentation, which use shall be limited to Licensee's internal use. The Software and Documentation are licensed, and not sold, to Licensee.

**3.2** Licensee may make one (1) copy of the Software for archival purposes. Licensee may use the Documentation only in connection with Licensee's use of the Software as authorized in Section 3.1 above. Licensee shall have no right to reproduce, modify, transfer, disclose, or distribute any Documentation.

**3.3** Licensee shall not, and shall not permit any third party to: (a) reverse engineer, disassemble, create derivative works and/or modify the Software; (b) except as specifically set forth below in section 3.4, assign, rent, lease, sell, transfer, or sublicense the Software; (c) electronically transfer or transmit the Software; (d) translate the Software into another computer language; or (e) copy or otherwise reproduce the Software or Documentation, other than as specifically authorized in this Section.

**3.4 Sublicense**

Licensee may sublicense the Software to another party provided that such sublicense is granted on the same terms and conditions as are set forth herein. It is the sole responsibility of the Licensee to obtain acceptance of these terms and conditions from any party to whom the Software is sublicensed.

In order to constitute a validly sublicensed copy, the Software must be reproduced in its entirety and without modification, including but not limited to any copyright notice, serial number, and any other notice affixed thereto.

**4. OWNERSHIP NOTICE**

**4.1** The Software and Documentation, and all intellectual property contained therein, are and shall remain the sole and exclusive property of Company and its licensors and are protected by copyright and trade secret laws and international copyright treaty provisions.

**4.2** Licensee shall not remove, modify, or in any manner tamper with any copyright, trademark or other proprietary notices embodied in the Software or on the Documentation, on any copy of the Software and Documentation, in any form, in whole or in part.

**5. WARRANTY DISCLAIMERS AND LIABILITY LIMITATIONS**

**5.1** COMPANY MAKES NO WARRANTY OR REPRESENTATION WITH RESPECT TO THE SOFTWARE AND IT IS LICENSED "AS IS" WITHOUT WARRANTY OF ANY KIND EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT, AND ANY STATEMENTS OR REPRESENTATIONS MADE BY ANY OTHER PERSON OR ENTITY ARE VOID. COMPANY MAKES NO REPRESENTATIONS THAT ANY PROGRAMMABILITY COMPLIES WITH THE APPLICABLE STATUTES, LAWS, OR REGULATIONS.

*© 2015*

**5.2** LICENSEE ASSUMES ALL RISK AS TO THE SELECTION, USE, PERFORMANCE AND QUALITY OF THE SOFTWARE. IN NO EVENT WILL COMPANY OR ANY OTHER PARTY WHO HAS BEEN INVOLVED IN THE CREATION, PRODUCTION OR DELIVERY OF THE SOFTWARE BE LIABLE FOR SPECIAL, DIRECT, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING LOSS OF PROFITS OR INABILITY TO USE THE SOFTWARE, EVEN IF COMPANY OR SUCH OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

**5.3** Some states and/or countries do not allow limitations on how long an implied warranty lasts and some states and/or countries do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation and exclusion may not apply to Licensee. This warranty gives Licensee specific legal rights, and Licensee may also have other rights which vary from state to state and/or country to country.

**6. GENERAL**

**6.1** If any provision or portion of a provision of this Agreement is determined to be invalid or unenforceable, it shall be deemed to be revised to the extent necessary to make it enforceable, or omitted if necessary, and the remaining provisions of this Agreement shall remain in full force and effect.

**6.2** This Agreement is governed by and construed in accordance with the laws of the State of California, without regard to its conflicts of law principles. The parties to this Agreement hereby irrevocably consent to the personal jurisdiction of the state and federal courts located in San Diego, California to resolve any dispute or controversy related to this Agreement.

**6.3** This Agreement constitutes the entire agreement between the parties with respect to the subject matter hereof, and all prior agreements, representations, statements and undertakings are hereby expressly canceled.

**6.4** Neither party hereto shall be liable in any manner for failure or delay in fulfillment of all or part of this Agreement directly or indirectly owing to any causes or circumstances beyond its reasonable control.

**7. EXPORT CONTROL REGULATIONS**

Licensee acknowledges and agrees that none of the Software, Documentation or underlying information or technology may be installed or otherwise exported or re-exported (a) into (or to a national or resident of) Cuba, Iran, North Korea, Sudan, Syria and any other country to which the U.S. has embargoed goods; or (b) to anyone on the U.S. Treasury Department's List of Specially Designated Nationals or the U.S. Commerce Department's Table of Denial Orders. Licensee further represents and warrants that it is not located in, under the control of, or a national or resident of any such country or on any such list, and will not transfer the Software to any of the foregoing.

**8. U.S. GOVERNMENT RESTRICTED RIGHTS**

The Software is provided with RESTRICTED RIGHTS. The use, duplication, or disclosure by the Government is subject to restrictions as set forth in subdivision (c)(1)(ii) of The Rights in Technical Data and Computer Software clause at 52.227-7013.

**9. INCLUDED SOFTWARE**

This product can be configured to use QuickTime software; Copyright 2009 Apple Inc., All rights reserved. This product can be configured to use VLC media player software, Copyright VideoLAN team, All rights reserved. This product uses wxWidgets software; Copyright 1998-2005 Julian Smart & Robert Roebling et al. This product can be configured to use FFmpeg software, Copyright FFmpeg project.

## Legal Disclaimer

The manufacturer provides this manual "as is," makes no representations or warranties with respect to its contents or use, and specifically disclaims any expressed or implied warranties of merchantability or fitness for any particular purpose. The manufacturer reserves the right to make changes to the content of this manual, at any time, without obligation to notify any person or entity of such changes.

The software described in this document is furnished under a license agreement. The software may be used or copied only in accordance with the terms of the agreement. It is against the law to copy the software on any medium except as specifically allowed in the license agreement.

No part of this manual may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's personal use, without the express written permission of the manufacturer.

© SoleraTec 2015. All Rights Reserved. Printed in the United States of America.

# Contact Information

Please contact us with any comments or suggestions regarding how we can improve our products or documentation. In your message to us include the name, version and comments about the product or guide, and also leave your name, phone number, or e-mail so we can contact you for clarifications.

## SoleraTec LLC

Website: www.SoleraTec.com

E-mail: sales@SoleraTec.com

Phone: 760.743.7200 Ext.109

Address: 2430 Auto Park Way Suite 205, Escondido, CA 92029

# Documentation Overview

## Notes about this guide

**Screenshots** - The screenshots in this guide are taken from a Windows operating system. Depending on the operating system you are running, the appearance of the applications may vary slightly, but the functionality is the same.

If viewing Help online, click a screenshot image to enlarge the display, and then click again to return its display to original size.

**Blue Text** - Blue text that is a topic heading can be clicked to expand for details when Help is being viewed online. Other blue text can be clicked to follow a link to another page in Help or to a website.

**Symbols** - This guide uses icon symbols to easily identify information.

= Indicates a useful tip.

= Indicates a warning statement.

**Path names** - The sample paths in this guide are for a Windows operating system. Depending on the operating system you are running, use the appropriate naming convention.

Paths for hard disk media, log files, and miscellaneous directories are case sensitive on non-Windows computers. Unless otherwise noted, when searching for a file or when creating a Vault, values typed are not case sensitive but are case preserving (the application ignores the case).

When entering paths, only use the forward slash (/) as a path name delimiter. You may get unexpected results if a backslash is used.

**Privileged Users** - Privileged users have rights to override security in the application as it relates to Phoenix RSM resources (media, stored data, vault operations), but do not have rights to override local computer security. The following are privileged users:

- Windows "Administrators" group
- Windows "Backup Operators" group
- Windows "Domain Administrator" user
- Windows "Domain Admins" group
- POSIX "root" user (UID:0)
- POSIX "root" group (GID:0)

**Unsupported naming conventions in Windows** - Some Windows applications create filenames with characters that are unreadable by Windows Explorer. These files are also unreadable by Phoenix RSM clients.

© 2015

**Note -** All features and functions discussed in this guide may not be available for your version of Phoenix RSM.

# Hardware and Software Requirements

To deliver advanced data management for Windows, Mac, Linux, and mixed environments, be sure to have at least the minimum or better of the following system requirements.

- Processes do not run optimally if hardware does not meet or exceed requirements.
- The interface appearance varies slightly depending on the platform used. For example, where a Window's menu displays **Exit**, a Mac menu displays **Quit**.

Regardless of your operating system, a keyboard, monitor, and mouse pointer is needed to properly run the software. If you are using a single-button mouse, press CTRL and click where the documentation states right-click.

## Windows

### Server:

**Windows Requirements**: Windows Server 2003 SP2; Windows XP SP3; Windows Vista SP2 (32-bit and 64-bit); Windows 7 SP1 (32-bit and 64-bit); Windows Server 2008 SP1 (32-bit and 64-bit); Windows Server 2008 R2 SP1; Windows 8 (32-bit and 64-bit); Windows 8.1 (32-bit and 64-bit); Windows Server 2012 (32-bit and 64-bit), Windows Server 2012 R2 (64-bit).

**Processor Requirements**: Intel i5 Core 3.00 GHz or better.

**Hard Drive Requirements**: 20 GB of available space to install and run the product.

**Memory Requirements**: 8 GB of RAM.

**Third party Requirements**: None.

### Client:

**Windows Requirements**: Windows Server 2003 SP2; Windows XP SP3; Windows Vista SP2 (32-bit and 64-bit); Windows 7 SP1 (32-bit and 64-bit); Windows Server 2008 SP1 (32-bit and 64-bit); Windows Server 2008 R2 SP1; Windows 8 (32-bit and 64-bit); Windows 8.1 (32-bit and 64-bit); Windows Server 2012 (32-bit and 64-bit), Windows Server 2012 R2 (64-bit).

**Processor Requirements**: Intel Dual Core 2.20 GHz or better.

**Hard Drive Requirements**: 10 GB of available space to install and run the product.

**Memory Requirements**: 4 GB of RAM.

© 2015

**Third party Requirements**: Latest version of Apple QuickTime 7 and supported codecs to allow playing of the video with which you are working. **Supported audio codecs:** X-QT, X-QUICKTIME, PCMU, GSM, PCMA, MPEG4-GENERIC, MP4A-LATM. **Supported video codecs:** X-QT, X-QUICKTIME, H263-1998, H263-2000, H264, MP4V-ES; VideoLAN media player (VLC 2.2.1 or newer); or some other video viewer.

## Mac

### Server:

**Apple Requirements**: Mac OS X 10.8.5 or newer.

**Processor Requirements**: Intel i5 Core 3.00 GHz or better.

**Hard Drive Requirements**: 20 GB of available space to install and run the product.

**Memory Requirements**: 8 GB of RAM.

**Third party Requirements**: None.

### Client:

**Apple Requirements**: Mac OS X 10.8.5 or newer.

**Processor Requirements**: Intel i5 Core 3.00 GHz or better.

**Hard Drive Requirements**: 10 GB of available space to install and run the product.

**Memory Requirements**: 4 GB of RAM.

**Third party Requirements**: Latest version of Apple QuickTime 7 and supported codecs to allow playing of exported video. **Supported audio codecs:** X-QT, X-QUICKTIME, PCMU, GSM, PCMA, MPEG4-GENERIC, MP4A-LATM. **Supported video codecs:** X-QT, X-QUICKTIME, H263-1998, H263-2000, H264, MP4V-ES; VideoLAN media player (VLC 2.2.1 or newer); or some other video viewer.

## Linux

### Server:

**Linux Requirements**: Red Hat 7.2 or newer; Fedora Core 12 or newer.

**Processor Requirements**: Intel Dual Core 2.20 GHz or better.

**Hard Drive Requirements**: 20 GB of available space to install and run the product.

**Memory Requirements**: 4 GB of RAM.

**Third party Requirements**: None.

© 2015

### Client:

**Linux Requirements**: Red Hat 7.2 or newer; Fedora Core 12 or newer.

**Processor Requirements**: Intel Pentium IV 3.40 GHz or better.

**Hard Drive Requirements**: 10 GB of available space to install and run the product.

**Memory Requirements**: 2 GB of RAM.

**Third party Requirements**: None.

### Network:

Multicast packet routing is required between all server and client machines.

### Vault Disk Storage:

**Disk-only:** Vault Storage is required on all servers. In case of disk-only configurations, sufficient storage must be provided to store all original video for the required retention period.

**Disk and Digital Data Tape:** In a mixed storage environment of disk and digital data tape, sufficient disk storage must be provided to store original video for period which it is required to be stored on disk. Additional disk storage must also be provided to store the Low Resolution Companion files and Thumbnails. This amount is normally equal to 10% of the total digital data tape storage capacity.

### Database Disk Storage:

Database storage requirements vary based on the amount of stored video and the use of metadata. Each server has its own database which correlates to the video it is storing. As a guideline, every 16 TB video storage will require 10 GB of disk storage as a minimum for the database.

For assistance in determining the amount of storage needed, please consult your Phoenix RSM sales agent.

### 3rd Party VMS Integration:

**Milestone/OnSSI:** For minimal CPU load impact to the Milestone/OnSSI image server, the recording server should be configured to record in JPEG mode.

**exacqVision:** No special requirements.

**Genetec:** No special requirements.

## Hardware Storage Configurations Supported

Phoenix RSM Vaults support several types of storage hardware, such as the following:

### Hard Disk

© 2015

When a hard disk based Vault is set up, Phoenix RSM uses an assigned portion of a computer's file system disk space. Space in this dynamic media environment can be added or removed very easily using the media management tools in Vault Admin.

### Data tape Stackers, Changers, Auto-loaders, and Libraries

A digital data tape system is a single unit of equipment with one or more data tape drives and internal shelves or slots where media is stored. These data tape automation systems contain robotics that move media between storage slots and the drives. They range from single drive systems, with a few tape slots, to large systems that can accommodate over 100 drives and thousands of data tapes.

Stackers and changers are sequential automation systems, designed to change data tapes in a sequence, from 1 through x. Auto loaders and libraries move media as tasked by the host system. Small Computer System Interface's (SCSI) are used to connect devices together.

### Single, "standalone" Data Tape Drives

This device manages a single data tape at a time without using robotics.

See also Installation and Product Licensing.

# Product Licensing

Get started with Phoenix RSM by purchasing a product license. You can purchase a regular licensed product online or download a trial version from SoleraTec's website.

## Product License

Product licensing is based on storage capacity and the number of cameras associated to a recording computer. The recording computer and server can be on the same or different boxes. Each Vault within your Information Repository requires a storage license to store video and every recording computer requires a camera license to record video.

Licenses for your products are tied to the computer where they were activated. You can move licenses between computers by requesting a new product key. Optional available licensed uses include: Data Service Policies, Vault platform devices, surveillance, or module extensions (Milestone, OnSSI, exacqVision).

The following is a breakdown of the two types of licensing:

- **Capacity licensing** – This license is used to increase Vault storage capacity for storing video, such as terabyte for hard disk storage or slot count for data tape storage device.
- **Camera licensing** – This license is used to allocate the number of cameras used to capture video per recording computer.

These licenses can be bundled together to achieve your needed storage capacity or camera count.

Run as many Phoenix RSM software clients as you need on the network at no additional charge.

## Evaluation License

© 2015

Phoenix RSM comes with a fully functional seven day evaluation license. At the end of the trial period you can either request an extended license or purchase a regular license through the same channels.

If you run the software longer than seven days with an evaluation license, your Vaults will shut down or your cameras will no longer be activated. Until a license is purchased and added, the Vaults run in increments of only two hours.

Your licenses are managed through Vault Admin. To activate or add a license, see Vault Properties License tab.

## Architectural Overview

SoleraTec's Phoenix RSM specializes in data storage and the management of your digital data assets. The data can be anything from document files to video files.

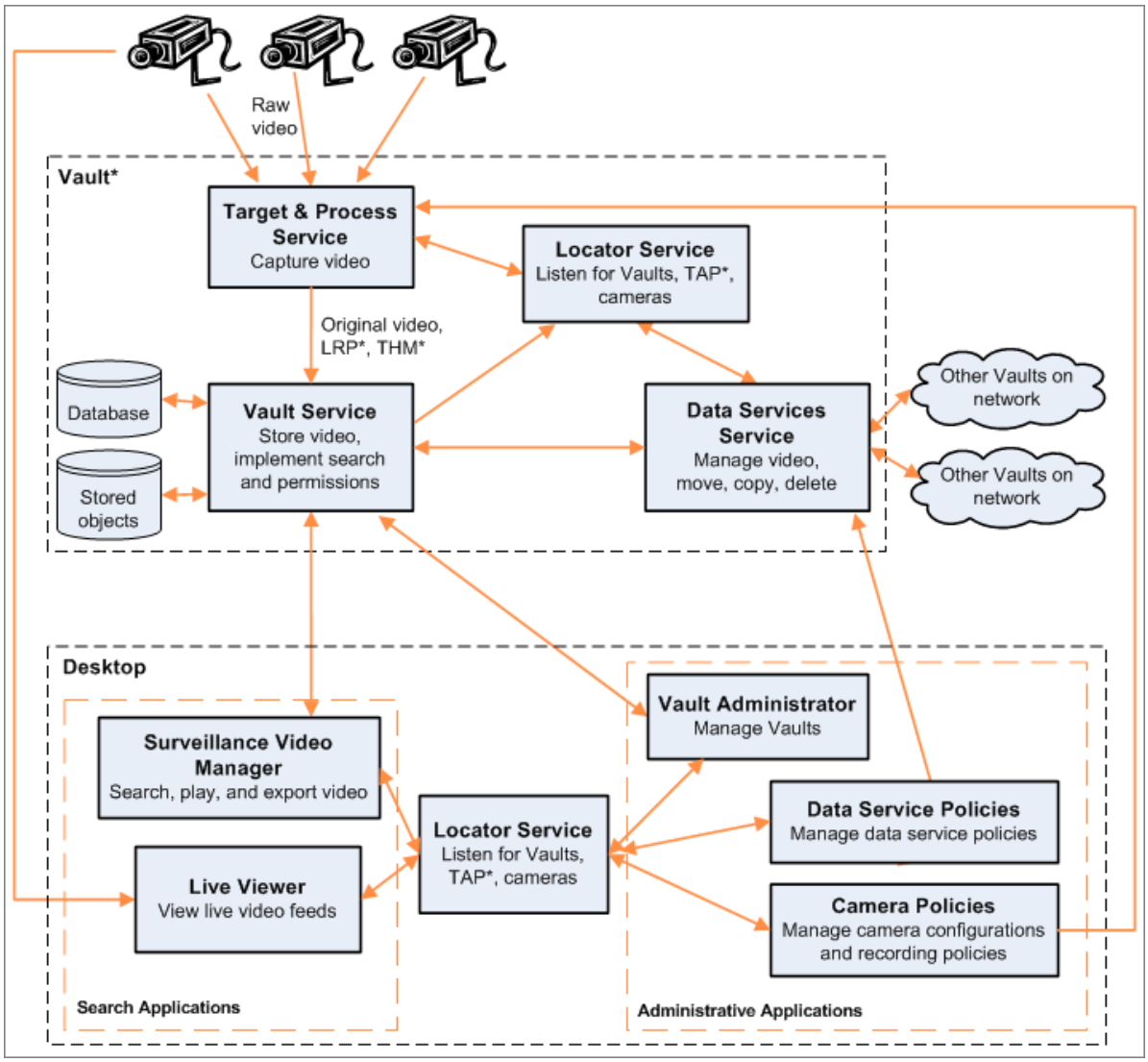
Phoenix RSM answers the call to your needs of:

- "I want to store data"
- "I want to move data around on my network"
- "I want to bring data back from storage to review or use"
- "I want to record and capture video"

This is not a disjointed system of data collection and then backup storage. It is a digital asset management solution which seamlessly integrates your data from video capture, to storage, and then immediate data retrieval - regardless of when or where stored.

The following diagram provides an overview of Phoenix RSM's architecture, illustrating how the different components of your solution work together. You can see how your digital data assets are captured or ingested into your Information Repository and are under complete management and never out of reach. Your assets can be searched on, moved around to different Vaults on the network, and retrieved in original quality for you to use.

© 2015




***Vault - Central processing unit, software, and storage device.**

***TAP - Target and Process.**

***THM - Thumbnail file.**

***LRP - Low resolution companion/proxy video.**

## Information Repository

The Information Repository is where data is stored. Since a Vault is a storage device used to store files, the Information Repository is made up of all the clients and Vaults on your network. The Information Repository can take many different forms depending on your needs and system, but it is flexible, easy to deploy, and is an active multi-tiered storage environment.

© 2015

In the Information Repository, data storage resources are virtualized as composite storage sets and operate as a federated environment. They can be comprised of a mixed set of networked data storage technologies running on Windows, Mac, Linux, and in mixed computing environments. If using Network Attached Storage (NAS) devices, then the Information Repository is all the networked units.

### The Word about Policies

Phoenix RSM employs the use of "policies" in most of its applications. They are the method outlined by parameters and options for managing all your digital assets effectively. As the user, you own the benefit of creating, customizing and executing these policies to fit your environment and workflow.

For more information see Technical Overview.

## Technical Overview

To use Phoenix RSM effectively, it is useful to understand its different components and how they interoperate to create a federated Information Repository. Phoenix RSM's balanced, extended client/server design provides advantages over technologies that rely on a client/server, client, or server component to drive and manage operations.

In a typical client/server model, clients are hard-coded to specific servers and cannot be changed without some manual interaction. Our extended client/server architecture includes a Locator Service, which dynamically locates and uses any storage resource available on the network as needed. This design proves advantageous over a traditional client/server model as it includes:

- **Automatic fail-over** - If there is more than one Vault available, clients can divide their use of the available Vaults. Clients fail-over from the current Vault in use to another Vault, should the current Vault fail.
- **Dynamic resource allocation** - Any network computer with Phoenix RSM installed can access storage resources on the network. An Information Repository can be comprised of many storage devices, based on whatever storage media and drive technology you want. Flexible parameters are configurable to send stored data to different storage devices based on the storage performance and longevity requirements. For more information see Locator Service.
- **Load balancing** - This is the distribution of jobs and data throughout the Information Repository. Phoenix RSM queries each Vault regarding the best match for processing requirements, storage resources, free space, and then establishes a connection to the Vault and copies files to the Vault. The network remains load balanced.

### Vault

The Vault concept makes the SoleraTec product unique and powerful. A Vault can be thought of as a storage container. On the server side, a Vault is comprised of a central processing unit (CPU), Phoenix RSM software, and storage. Each Vault requires its own product key because of its scalable possibilities.

© 2015

The Vault(s) on the network make up the Information Repository to manage all your data storage needs. The Vaults have attributes associated to them like licensing, media, and files, and are easy to upgrade. They are decentralized, making the Information Repository a distributed solution across your network - but overall data management remains centralized and under complete control. Phoenix RSM is truly a multi-tiered storage and digital asset management solution. For more information see Vault Admin.

## Components

Phoenix RSM includes server components and client components.

During the installation process you can opt to install the server or client but it is important to note that clients do not function unless a Phoenix RSM server has been installed on the network. For more information see Installation.

### Server

The server contains all the applications found in the client component, plus Vaults and administrative tools.

Server Vault applications are:

- **Vault Service** - The Vault service manages the Vault(s) on the network. The Vault uses storage space in a hierarchical manner, where each level is unique and features its own access control list and other parameters. This allows for load balancing, automatic fail-over, and for media to be targeted granularly for specific uses and across multiple devices.
- **Data Services Service** - Use to create policies for complete data lifecycle management in the Information Repository. This service provides an easy way to migrate, replicate, or purge data between Vaults and ensure that data is preserved or maintained on media within a storage hierarchy.
- **Target and Process Service** - This service ingests data into the Information Repository and metadata is extracted from the data and cataloged in databases.
- **Add Remove Vault Wizard** - Use to add or remove a hard disk Vault, standalone data tape Vault, or a data tape library Vault.

With the server set up, you can optionally select the following server administration tools:

- **Camera Policies** - Add cameras and create camera policies that capture live video feeds automatically on a scheduled basis.
- **Vault Admin** - Prepare media and manage media in the Information Repository Vaults.
- **Data Service Policies** - Create data services policies to manage the data lifecycle within the Information Repository. The data services policies can classify, collate, and consolidate data automatically. Easily migrate, replicate, or purge data between Vaults and ensure that data is preserved or maintained on media within a storage hierarchy.

Tasks the server manages are: the Locator Service, finding and connecting to available Vaults, receiving, locating, storing content and metadata to and from Vaults, and SHA256 checksum (digital fingerprinting).

© 2015

## Client

The client contains all of the applications found in the server component except Vaults and administrative tools. It can run on any computer that is not running Phoenix RSM servers.

Client functionality can be run from the executables from your suite of product applications. Each application plays a role in your complete digital asset management solution. All Phoenix RSM applications are easy to use, and include many features to customize job parameters and schedules. The clients operate independently of servers and Vaults.

Client applications are:

- **Live Viewer** - View and record live video feeds from RTSP-enabled IP cameras.
- **Surveillance Video Manager** - Use to search, review, and export video (and metadata) managed in the Information Repository to any computer on the network.
- **Video Components Generator** - The video components generator specifies the quality for the picture thumbnail.
- **Locator Service** - The Locator is an essential component of communication to run any Phoenix RSM application, it enables the dynamic resource allocation, and it keeps the Information Repository current regardless of how large the environment is.
- **Network Activity** - Use to monitor all data, media, and vault operations within the Information Repository in real-time.

Tasks the client applications manage are: searching digital assets for capture, ingest and moving assets within the Information Repository, communicating with servers for storage resources, digital fingerprinting validations, error and activity logging, and video file location and retrieval.

## Administrative Control

Along with Phoenix RSM applications, a suite of command line executables are available for managing the Information Repository. When a window-based session is not available, the command lines can be used for scripting and running Phoenix RSM. Use the command line interface only if you are an advanced user of Phoenix RSM and are familiar with command line environments.

Access to any Phoenix RSM functionality can be controlled fully by the system administrator. Access to sensitive activities within the Information Repository, such as installing, opening, securing, and de-securing Vaults, requires administrator level access. This allows administrators to determine who has permissions to management functionality.

Administrators can limit access to functionality as follows:

- Client access for users.
- Protecting clients. By default, policies can be modified only by administrators.

When changing rights, exercise caution because services that use policy files normally run at an elevated privilege level and have access to data to which the typical user may not have rights.

© 2015

- Setting rights on media. If a user does not have read access to a media, then no search/retrieve from media is granted. If a user does not have write access to media, then the user cannot ingest data to media.

Similar to the setting of rights, most of the functionality that is set by default in Phoenix RSM can be modified to meet your unique ILM requirements.

### Extensibility

Phoenix RSM is equipped with resources to incorporate pre-processing or post-processing scripts into storage, migration, replication, and purge policies. It is also equipped with internal APIs to link the storage management engine to other front-end or back-end applications.

### Command Lines

From your suite of product applications, there are application executable files and dynamic link library files (.dll). Notice that some of the executable files have a "Cl" at the end of the name - for example, VaultAdminCl.exe.

The "Cl" stand for command line. If you click the "Cl" version application executable, the application runs via a terminal. This functionality is intended for advanced users to do scripting or diagnostic work within the application.

In addition, there are services that are running all the time in the background. The command line arguments that you can work with are application startup arguments for advanced users to perform diagnostics on the program.

For more information see Command Line Arguments.

## Installation

This topic provides information, tips, and how to's on installing SoleraTec's Phoenix RSM.

Before installation, make sure your computer meets minimum system requirements.

There are a few differences to understand between the Server Bundle and the Client Bundle. The main difference between the Phoenix RSM Server Bundle and Client Bundle is that the Server Bundle includes Phoenix RSM Vaults and administrative tools. You should install the Server Bundle on computers you want Vaults to reside. Install the Client Bundle on computers you want only clients to run.

Here is a brief breakdown of each bundle:

**Server Bundle**

- Does not have to run on a server.
- Must be installed first on your network, otherwise the Client Bundle will not function.

© 2015

- Includes all of the components contained in the Client Bundle. Because of this, do not install the Server and Client Bundle on a single computer.
- Install on computers that are to have Vaults.

For optimal performance, install the Server Bundle local to the Vaults they are to manage.

**Client Bundle**

- Install just the Client Bundle on other computers on the network after you have installed the Server Bundle somewhere on your network.
- Install on computers that do not contain Vaults.

## Install

See the appropriate section for the platform to install your Phoenix RSM. Uninstall instructions are included as well.

- Windows
- Mac
- Linux

After installation is complete, the next step is to add Vaults. See Add or Remove Vault Wizard. For more information about what's next, see Getting Started.

## Important Installation tips

- To install, you need to have administrative permissions.
- Phoenix RSM must be installed on a NTFS partition, not a FAT32 partition. This is especially true for Mac Boot Camp Windows installations as the default partition is FAT32.
- Phoenix RSM Vaults and surveillance video ingest servers require running on a computer configured to use static IP address assignment. Using DHCP to obtain a dynamic IP address may result in unpredictable system behavior.

### Network Connectivity Requirement

Phoenix RSM is designed to run on a network. Running it on a computer that is not networked causes unexpected performance. If you need to run it on a standalone Windows computer, you must use the Microsoft Loopback adapter bundled in Windows to create a virtual network environment. Go to http://support.microsoft.com/kb/839013 for details.

### Firewall Rights Requirement

© 2015

Most firewalls are pre-configured to block most programs from communicating to maintain a high level of security. Your local firewall software on the computer where Phoenix RSM is installed may interfere with Phoenix RSM operations.

If you are running a local firewall, make sure all Phoenix RSM components have pass through rights to at least the locally connected network or networks. Refer to your operating system documentation regarding how to unblock Phoenix RSM from communicating.

### Date and Time Properties on Computers with Vaults

All computers in the Information Repository that contain Vaults and any VMS system that video is captured from must be synchronized to the same time source for the Information Repository to function correctly.

### Multicast

Phoenix RSM uses multicast and beacon technology to communicate between clients, Vaults, and available Phoenix RSM services. The default Phoenix RSM multicast address is 224.0.23.160.

## Server Bundle and Client Bundle Contents

When you install the DVD or launch the installation executable, you are given the option of installing a Server Bundle or a Client Bundle. If you select to install the Client Bundle, only a subset of the applications in the Server Bundle are installed.

Applications listed below that end with "CI" and "Svc" are run from a command line.

The Server Bundle and Client Bundle include the following:

| Module | Contents | Server | Client |
|---|---|---|---|
| **Help** | Browser based (HTML) help | Yes | Yes |
| **Documentation** | PDF based documentation | Yes | Yes |
| **Administration** | Applications for administration and Information Repository monitoring, including:<br>• Vault Admin<br>• Network Activity<br>• Locator Admin Command Line Interface (LocAdminCI)<br>• Vault Admin Command Line Interface (VaultAdminCI) | Yes | Yes |

© 2015

| Module | Contents | Server | Client |
|---|---|---|---|
| **Surveillance Video Manager** | A visual interface that enables users to search for surveillance video files in the Information Repository. Also export selected clips or entire files to any computer on the network. | Yes | Yes |
| **Camera Policies** | Add cameras, capture video feeds, on a scheduled basis from RTSP enabled IP cameras. | Yes | Yes |
| **Live Viewer** | View Live feeds from any RTSP-enabled IP camera that is on the network. Cameras must first be configured using Camera Policies. | Yes | Yes |
| **Data Services** | Applications for migrating, replicating, and purging data in the Information Repository, including:<br>• Data Service Policies<br>• Data Services Command Line Interface (DataSvcsCl)<br>• Data Services Service (DataSvcsSvc). | Yes | Yes |
| **Vault** | The Vault services applications:<br>• Vault Service (VaultSvc)<br>• Add or Remove Vault Wizard | Yes | No |

# Windows

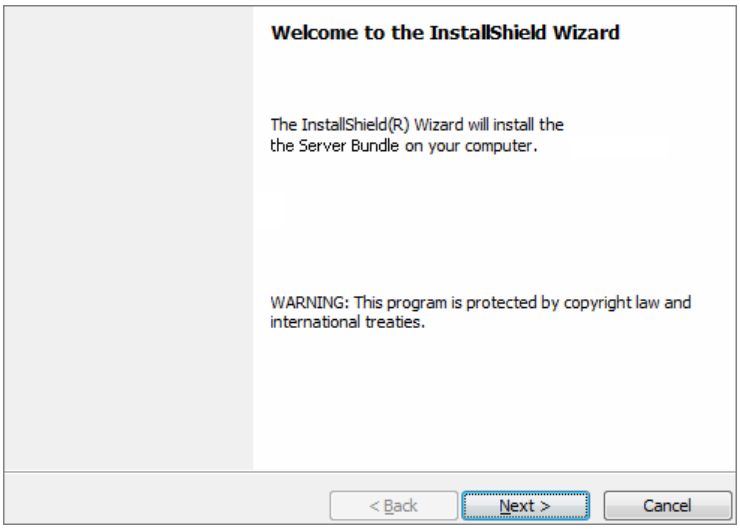
Perform the following steps to install on the Windows operating system (OS). The appearance of your screens may vary slightly from those shown here depending on your Phoenix RSM version and your OS.

Installation is quick and easy and done through an InstallShield Wizard. Each wizard dialog box includes **Back**, **Next**, and **Cancel** buttons. The **Back** button navigates you back to the previous dialog box (except on the Welcome window), and the **Next** button accepts current values and advances you to the next window in the wizard. The **Cancel** button closes the wizard without saving values. The **Finish** button appears on the last wizard window to complete the process.

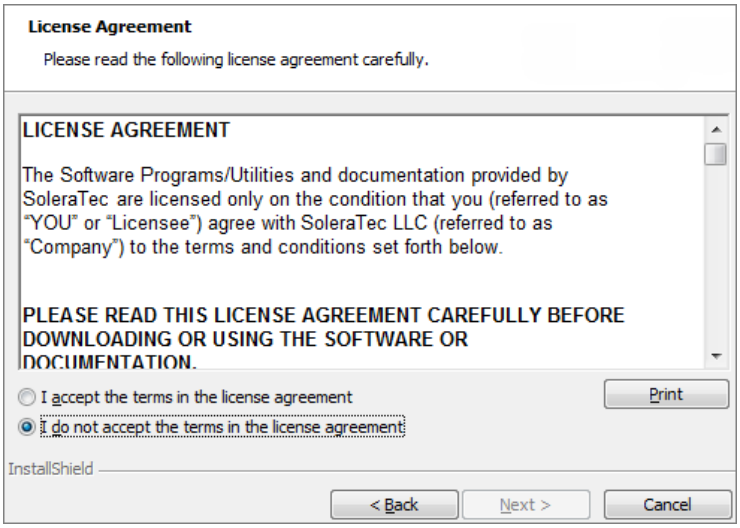
## Server Bundle for Windows

1. Click the application executable (from your installation disc or installation folder).

© 2015


Welcome to the InstallShield Wizard
The InstallShield(R) Wizard will install the
the Server Bundle on your computer.
WARNING: This program is protected by copyright law and
international treaties.
< Back
Next >
Cancel

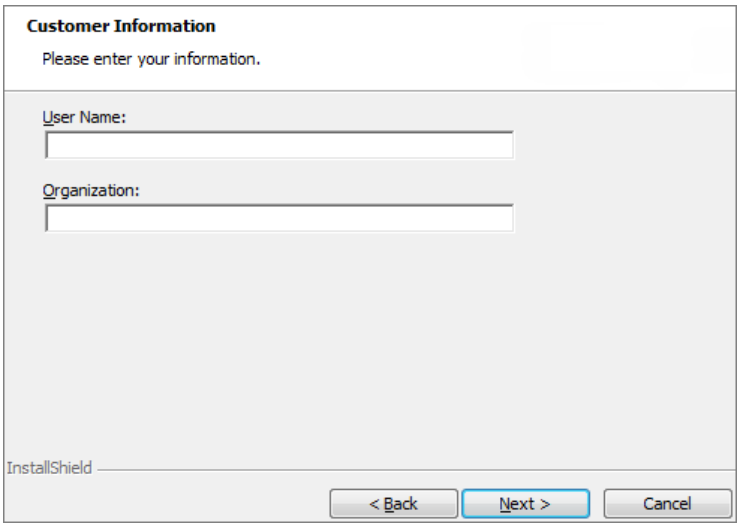
2. Select **Next** to review the software license agreement.


License Agreement
Please read the following license agreement carefully.
LICENSE AGREEMENT
The Software Programs/Utilities and documentation provided by
SoleraTec are licensed only on the condition that you (referred to as
"YOU" or "Licensee") agree with SoleraTec LLC (referred to as
"Company") to the terms and conditions set forth below.
PLEASE READ THIS LICENSE AGREEMENT CAREFULLY BEFORE
DOWNLOADING OR USING THE SOFTWARE OR
DOCUMENTATION.
I accept the terms in the license agreement
I do not accept the terms in the license agreement
Print
InstallShield
< Back
Next >
Cancel

3. Read the license agreement, and if you accept the terms, select **I accept the terms in the license agreement**.

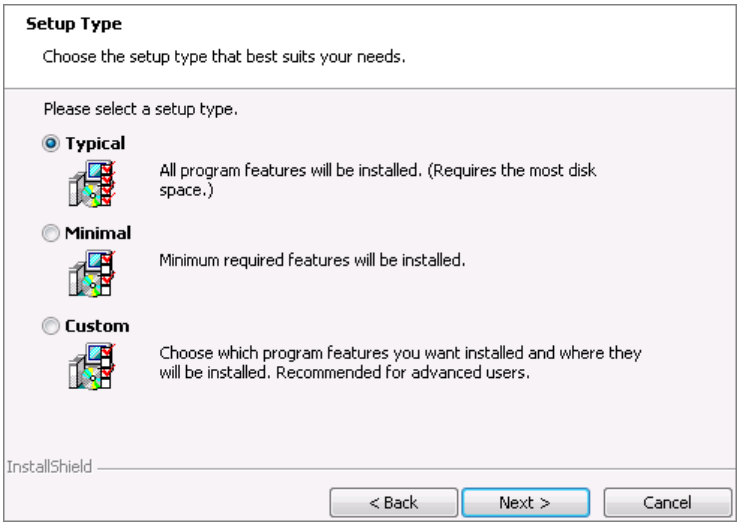
4. Select **Next** to enter your customer information.

© 2015




5. Type your **User Name** and **Organization**.

6. Select **Next** for the setup type.


Setup Type
Choose the setup type that best suits your needs.
Please select a setup type.
Typical
All program features will be installed. (Requires the most disk space.)
Minimal
Minimum required features will be installed.
Custom
Choose which program features you want installed and where they will be installed. Recommended for advanced users.
InstallShield
< Back
Next >
Cancel

8. Select the type of Server installation you prefer. Typical is recommended:

   **Typical** - A complete installation. See Server Bundle contents.

   **Minimal** - Includes everything in Typical except Help and Documentation.

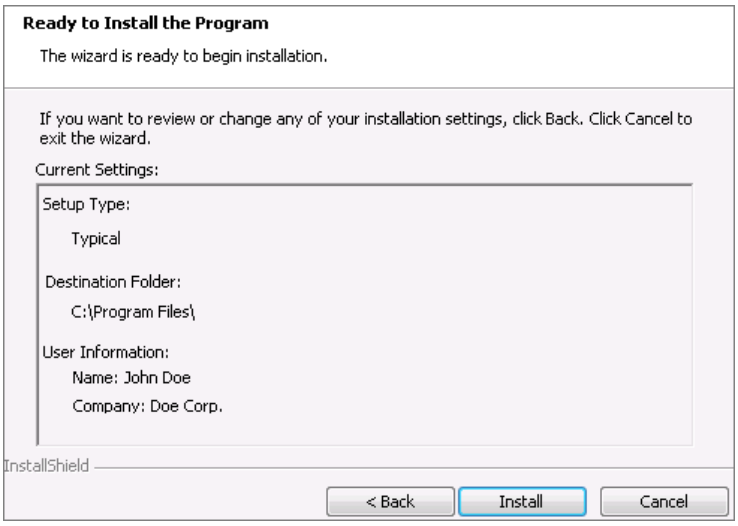
   **Custom** - By default, includes everything in Typical. If you select **Custom**, click **Next** for the Custom Setup window to appear. To select which components are to be installed click the Help drop-down icon for a list of feature options.

   The Custom Setup window also includes the following option:

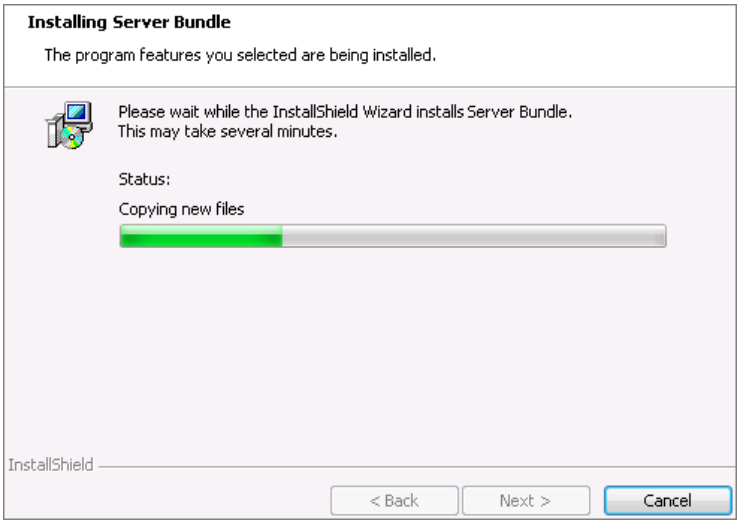
   - **Space** launches the Disk Space Available window, displaying the amount of disk space required to install selected features. The window also highlights any volumes that do not have enough disk space to support the selected features.

© 2015

9. After you have made your selection, select **Next** to review.

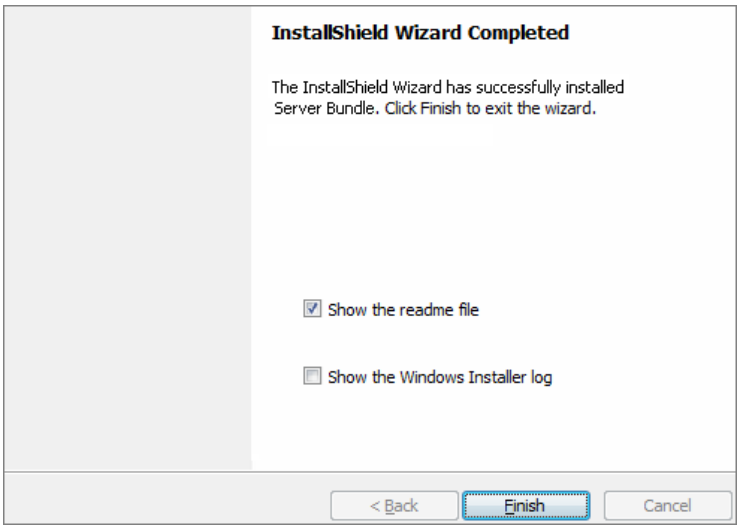



10. Review the summary of installation in the Ready to Install the Program window. If all the information looks correct, click the **Install** button and the Installing Server Bundle window displays.


Installing Server Bundle
The program features you selected are being installed.
Please wait while the InstallShield Wizard installs Server Bundle. This may take several minutes.
Status:
Copying new files
InstallShield
< Back
Next >
Cancel

11. When the installation is complete, the InstallShield Wizard Completed window presents you with the options to see the readme file and log.

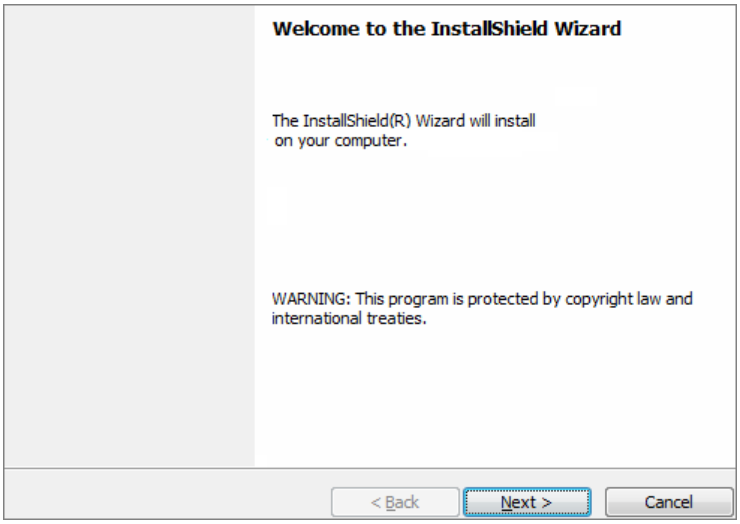
© 2015


InstallShield Wizard Completed
The InstallShield Wizard has successfully installed Server Bundle. Click Finish to exit the wizard.
Show the readme file
Show the Windows Installer log
< Back
Finish
Cancel

12. Click the **Finish** button to complete the process.

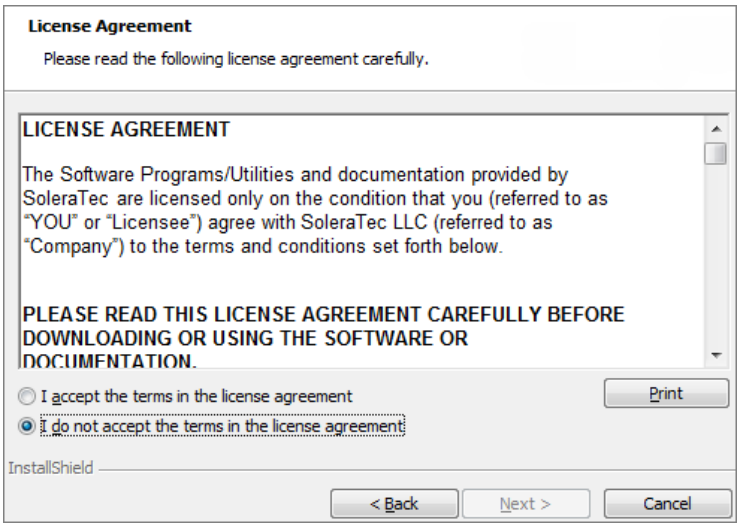
## Client Bundle for Windows

1. Click the application executable (from your installation disc or installation folder).


Welcome to the InstallShield Wizard
The InstallShield(R) Wizard will install on your computer.
WARNING: This program is protected by copyright law and international treaties.
< Back
Next >
Cancel

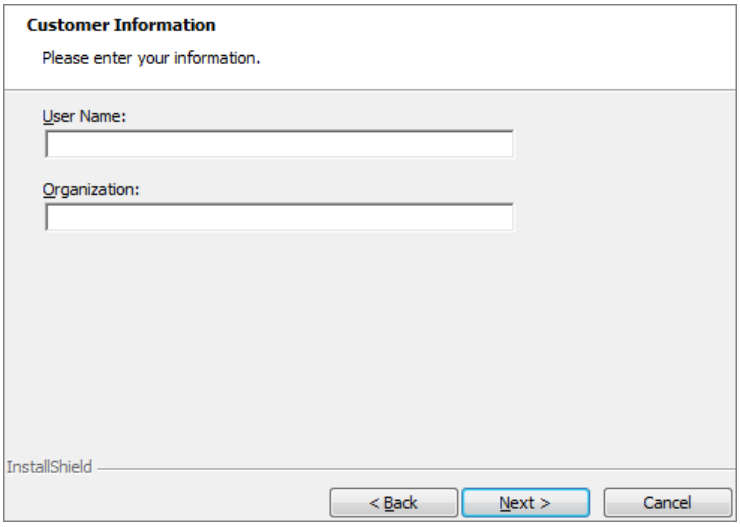
2. Select **Next** to review the software license agreement.

© 2015


License Agreement
Please read the following license agreement carefully.
LICENSE AGREEMENT
The Software Programs/Utilities and documentation provided by SoleraTec are licensed only on the condition that you (referred to as "YOU" or "Licensee") agree with SoleraTec LLC (referred to as "Company") to the terms and conditions set forth below.
PLEASE READ THIS LICENSE AGREEMENT CAREFULLY BEFORE DOWNLOADING OR USING THE SOFTWARE OR
I accept the terms in the license agreement
I do not accept the terms in the license agreement
Print
InstallShield
< Back
Next >
Cancel

3. Read the license agreement, and if you accept the terms, select **I accept the terms in the license agreement**.

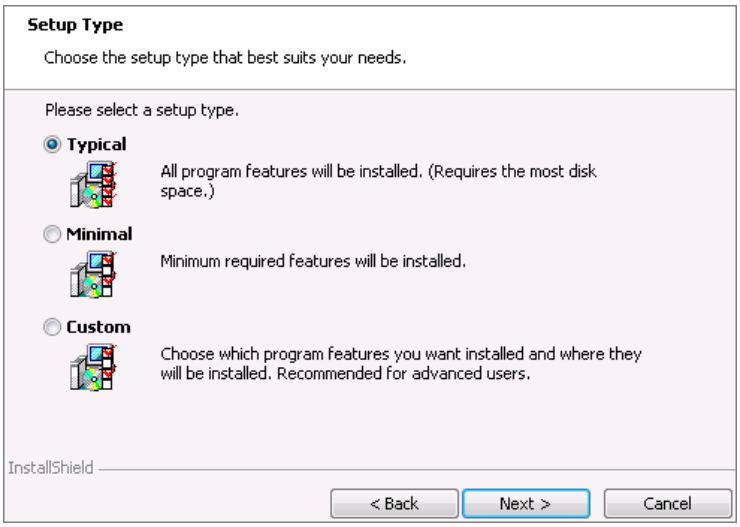
4. Select **Next** to enter your customer information.




5. Type your **User Name** and **Organization**.

6. Select **Next** to select a setup type.

© 2015


Setup Type
Choose the setup type that best suits your needs.
Please select a setup type.
Typical
All program features will be installed. (Requires the most disk space.)
Minimal
Minimum required features will be installed.
Custom
Choose which program features you want installed and where they will be installed. Recommended for advanced users.
InstallShield
< Back
Next >
Cancel

7. Select the type of installation you prefer. Typical is recommended:

   **Typical** - A complete installation. See Client Bundle contents.

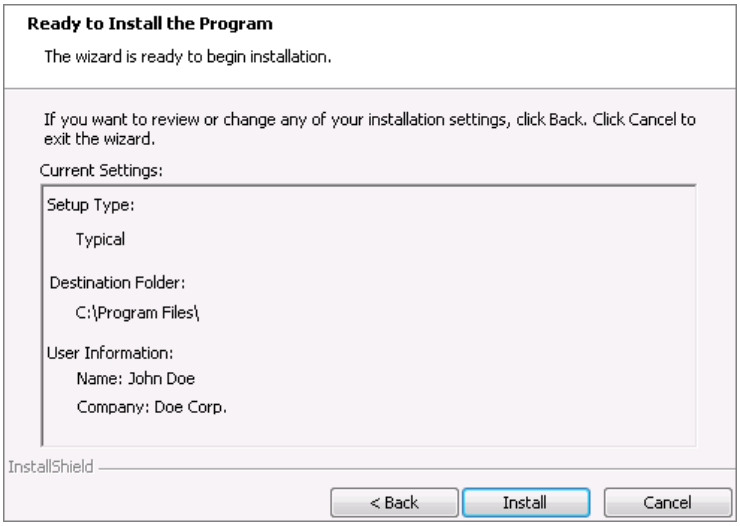
   **Minimal** - Includes everything in Typical except Help and Documentation.

   **Custom** - By default, includes everything in Typical. If you select **Custom**, click **Next** for the Custom Setup window to appear. To select which components are to be installed click the Help drop-down icon for a list of feature options.

   The Custom Setup window also includes the following option:

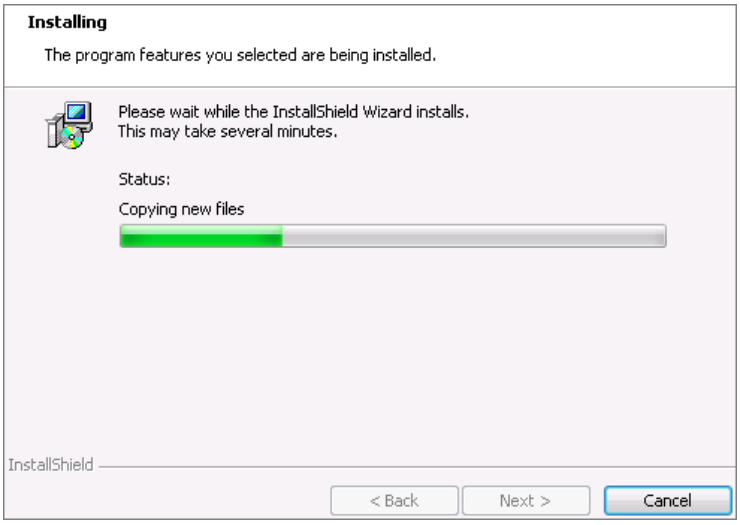
   - **Space** launches the Disk Space Available window, displaying the amount of disk space required to install selected features. The window also highlights any volumes that do not have enough disk space to support the selected features.

8. After you have made your selection, select **Next** to review.

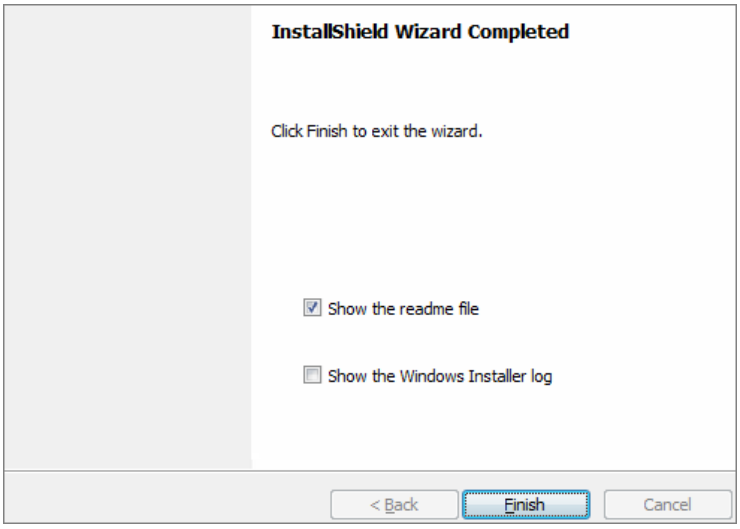



© 2015

9. Review the summary of installation in the Ready to Install the Program window. If all the information looks correct, click the **Install** button and the Installing Client Bundle window displays.




10. When the installation is complete, the InstallShield Wizard Completed window presents you with the options to see the readme file and log.




11. Click the **Finish** button to complete the process.

After installation is complete, the next step is to add Vaults. See Add or Remove Vault Wizard. For more information about what's next, see Getting Started.

When updating a previous Phoenix RSM installation, all Phoenix RSM Services settings will be reset to installation defaults. If you made any changes to these settings in the prior installation, you may need to reapply your changes after the update completes.

## Uninstall from Windows

© 2015

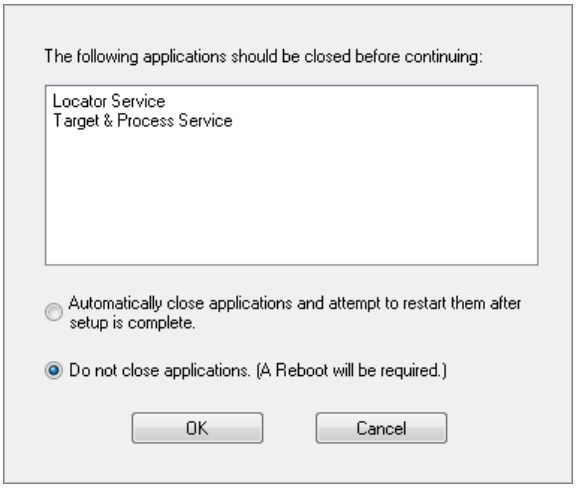
If you need to uninstall your Phoenix RSM from Windows, this can be easily done by following the steps below.

The uninstall process does not remove modified configuration files or files that were not in the installation, such as files that could have been added.

- Administrator rights are needed to uninstall Phoenix RSM.
- Before uninstalling Phoenix RSM, create a backup copy of any data that you do not want to lose.

1. Uninstall Phoenix RSM from your Windows computer just as you would any other Windows application.

When uninstalling Phoenix RSM from Windows, you might be asked whether to automatically close applications.


The following applications should be closed before continuing:
Locator Service
Target & Process Service
Automatically close applications and attempt to restart them after setup is complete.
Do not close applications. (A Reboot will be required.)
OK
Cancel

2. Select **Do not close applications (A Reboot will be required)**.

3. Reboot your computer once the Add/Remove Windows Programs is finished.

For more information see Installation.

# Mac

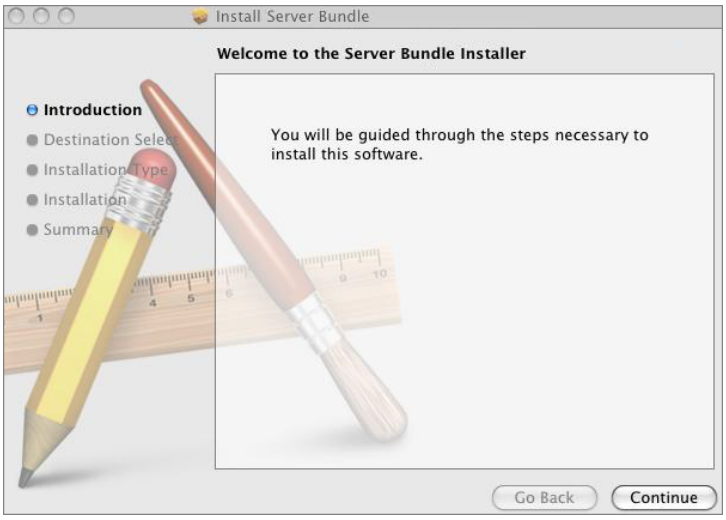
Perform the following steps to install on the Apple operating system. The appearance of your screens may vary slightly from those shown here, depending on your Phoenix RSM version.

Installation is quick and easy; done through an Install Wizard. Each wizard dialog box includes **Go Back** and **Continue** buttons. The **Go Back** button navigates you back to the previous dialog box (except on the Welcome window), and the **Continue** button accepts current values and advances you to the next window in the wizard. The **Install** button appears on the last wizard window to complete the process.

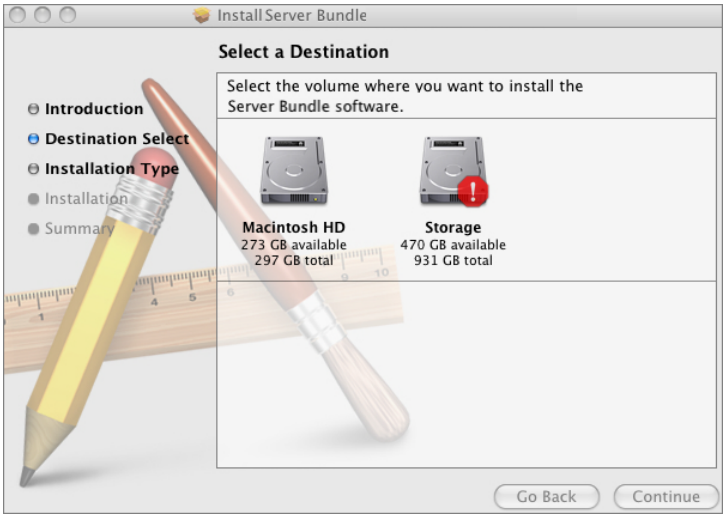
## Server Bundle for Mac

© 2015

1. Click the application executable (from your installation disc or installation folder).



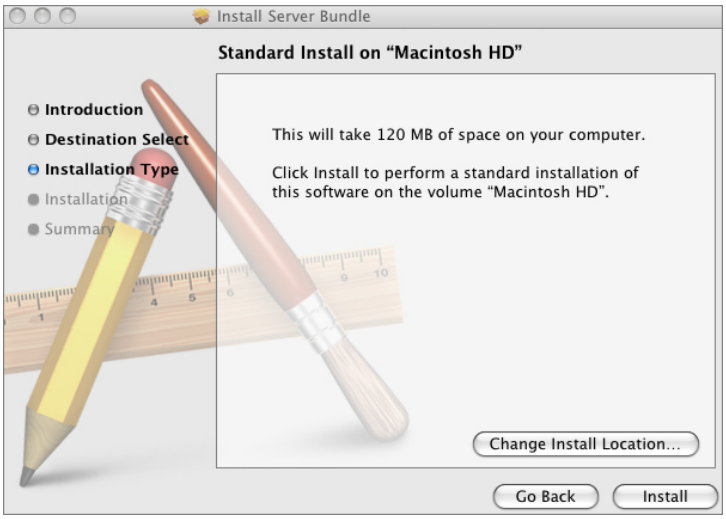

2. Select **Continue** for the Select a Destination window.




3. Accept the default destination for Phoenix RSM to be installed to.

4. Select **Continue** for the Installation Type window.

© 2015

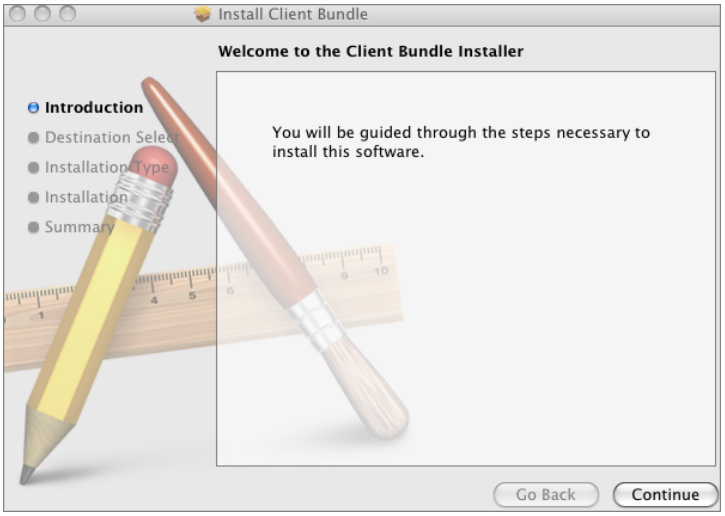



5. Click the **Install** button; the product installs.

6. When the installation is complete, restart your computer.

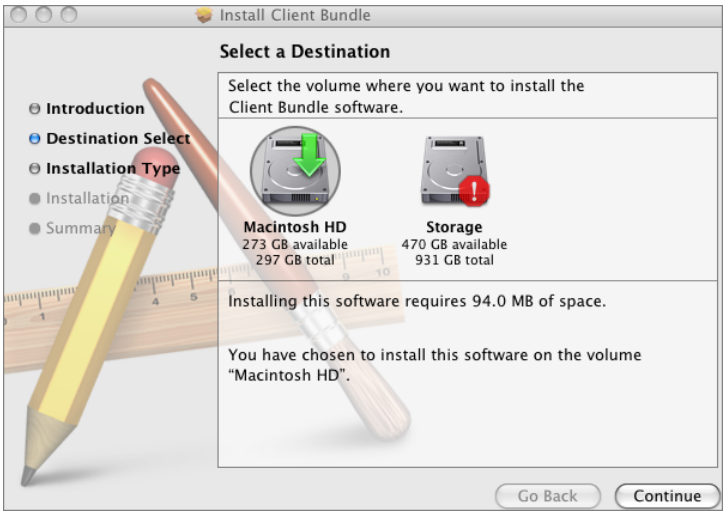
## Client Bundle for Mac

1. Click the application executable (from your installation disc or installation folder).

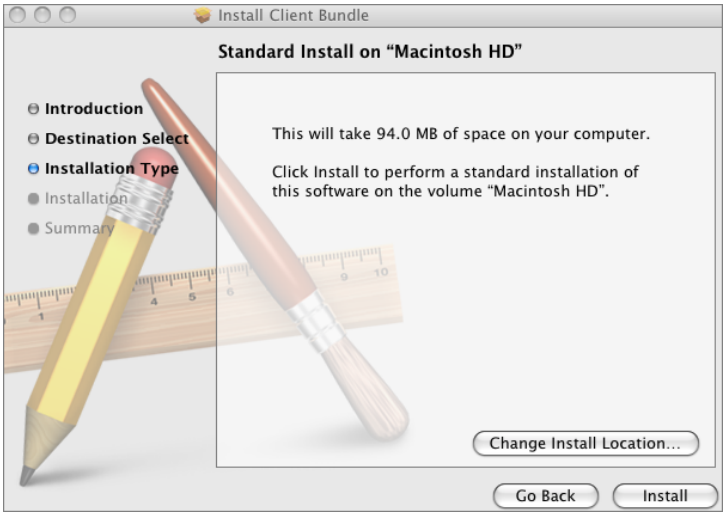



2. Select **Continue**. If you have multiple hard drives installed, the Select Destination window appears. Otherwise, skip to the Installation Type window.

© 2015




3. Accept the default destination for Phoenix RSM to be installed to.
4. Select **Continue** for the Installation Type window.




5. Click the **Install** button; the product installs.
6. When the installation is complete, restart your computer.

After installation is complete, the next step is to add Vaults. See Add or Remove Vault Wizard. For more information about what's next, see Getting Started.

## Uninstall from Mac

If you need to uninstall Phoenix RSM, this can be easily done by following the steps below.

© 2015

The uninstall process will remove configuration files and data that were not in the original installation and created while using Phoenix RSM. This may include databases and media storage. Be sure to move any files or folders in the Applications > Phoenix folder to a safe location before uninstalling the product.

- Administrator rights are needed to uninstall Phoenix RSM.

1. Go to Applications > Utilities and open a Terminal.
2. In the Terminal, type **sudo /Applications/Phoenix/Bin/Uninstall.sh** and press **Return**.
3. Enter the Admin password when prompted and press **Return**. When you type, the password will not be shown.
   - This will uninstall Phoenix RSM from your Mac computer.
4. Reboot your computer.

For more information see Installation.

# Linux

Perform the following steps to install on the Linux operating system.

## Server Bundle for Linux

1. Open **Setup.html** (from your installation disc or installation folder). Follow the directions to open the Phoenix RSM Server Bundle. The following appears:

```
Phoenix RSM Install Wizard, version x.x.x



Welcome to the Install Wizard for SoleraTec Phoenix RSM.



This Install Wizard will help you to install SoleraTec's Phoenix RSM version
x.x.x on your

computer. During the installation process, you will be asked where to
install Phoenix RSM

and which components to install. Choices appear in a comma separated list
with the default

choice in square brackets. Pressing the Enter key selects the default
choice.



To continue, press <Enter>
```

© 2015

2. Press ENTER. The following appears:

```
==============



The current location for Phoenix RSM is /usr/local/Phoenix. Would you like
to install

Phoenix RSM in its current location?

[(y)es] (n)o (b)ack (q)uit >[y]
```

From this point on, you have the option of using **b** to go back to any earlier point in the process and change your selection. You can also use **q** to quit the installation process and exit the wizard.

3. Type **y** to accept the default location. Or, type **n** to enter a new location. If you select **n**, you are prompted to enter the new installation directory location. After typing **y**, the following appears:

```
==============



Here is a list of the packages available for installation. Please indicate
the package you want to

install by entering the number beside your selection. Number 1 is the
default choice and will be

chosen if you simply press the Enter key.

1. Phoenix RSM Server package

[1], 2, (b)ack, (q)uit >[1]
```

4. Type **1** to select the Phoenix RSM Server Bundle. The following appears:

```
==============



You chose to install the Server package to '/usr/local/Phoenix'. Is this
correct?

[(y)es] (n)o (b)ack (q)uit >[y]
```

5. Type **y**. The following appears:

```
==============

As services are started, you may safely ignore any warning messages
```

© 2015

```
which specify "WARNING" or "No active vaults found"


Installing Phoenix RSM Server package
```

After installation is complete, the next step is to add Vaults. See Add or Remove Vault Wizard. For more information about what's next, see Getting Started.

### Uninstall from Linux

If you need to uninstall your Phoenix RSM from Linux, this can be easily done by following the steps below.

The uninstall process does not remove modified configuration files or files that were not in the installation bundle, such as log files or files that could have been added.

- Administrator rights are needed to uninstall Phoenix RSM.

- Before uninstalling Phoenix RSM, create a backup copy of any data that you do not want to lose.

1. Enter the following command at root (where Phoenix RSM was originally installed): Phoenix/Bin/uninstall.

2. Reboot your computer.

For more information see Installation.

# Getting Started

Getting started with SoleraTec's Phoenix RSM is easy. This section provides instructions on how to launch the Phoenix RSM applications, and then how to quickly get started with a basic Phoenix RSM workflow. The Quick Start will get you up and running, but it is the review of the topics of this User guide in addition to the Quick Start workflow that will help you become a master of your Phoenix RSM.

See Quick Start.

### Launch an Application

To launch an application, see the instructions under the operating system where you are running Phoenix RSM.

#### Windows

- From the Windows desktop, select Start > All Programs > Phoenix, and then select the application to run.

#### Mac

© 2015

- From the Mac desktop, browse to Applications > Phoenix > Bin, and then select the application to run.

## Linux

1. To launch a Phoenix application on Linux using a GNOME desktop, double-click Computer on the desktop.

2. Double-click File System > usr > local > Phoenix > Bin, and then double-click the executable to launch. (For other Linux desktops, this process is similar.)

    - Any executable that has "Svc" or "Cl" as part of its name is not an application.

The following are the applications in Bin to open. Depending on your product you may not see all the applications:

| Executable | Application |
|---|---|
| AddRemVltWzrd | Add or Remove Vault Wizard |
| CameraPolicies | Camera Policies |
| DataSvcPolicies | Data Service Policies |
| HostInfo | Host Information |
| NetActivity | Network Activity |
| SurveillanceVideoManager | Surveillance Video Manager |
| VaultAdmin | Vault Admin |

**Open with UNIX**:

When starting an application on Linux through a terminal shell using **cd /usr/local/Phoenix/Bin/...**, click the **X** button on the terminal shell to close the terminal and application. If you press CTRL+C, it aborts and the application closes. If you have not saved your policy, any new parameters are not saved.

To avoid closing an application inadvertently, start the application using the nohup command. Type ( **nohup ./VaultAdmin >/dev/null 2>&1 < /dev/null &**) at the prompt. This completely isolates the command from the parent terminal shell.

## Command Line with Windows

If using a command line, type the path, including the name of the executable for the client you want to launch. For example, type C:/Program Files/Phoenix/Bin/DataSvcPolicies.exe to launch Data Services Policies. Navigate to the directory that contains your Phoenix executables for available applications.

- Any executable that has "Svc" or "Cl" as part of its name is not an application.

© 2015

The following are applications to launch from a command line:

| Executable | Application |
|---|---|
| DataSvcPolicies | Data Services Policies |
| SurveillanceVideoManager | Surveillance Video Manager |
| VaultAdmin | Vault Admin |
| NetActivity | Network Activity |

# Quick Start

Now that you have SoleraTec's Phoenix RSM, let's get you up and running with it so you can begin to record, store, and manage surveillance video.

These instructional procedures cover a quick and easy setup for both RTSP-enabled IP camera users and VMS users. They provide a basis for subsequent workflows that you may encounter while using your product applications.

Follow the steps below.

## 1. Install Phoenix RSM

**To install the software from a CD-ROM**

a) Ensure that your computer is properly configured and connected to a network.

b) Insert the Phoenix RSM CD-ROM, and open Setup.html from your installation disc or folder.

c) Follow the directions to open and install the Phoenix RSM Server Bundle.

d) If running on Windows firewall settings are established automatically during the installation process. If running on a platform other than Windows ensure that Phoenix RSM is not blocked by the firewall on your local computer.

**To install the software from the website**

a) Go to SoleraTec's website and click **Download**.

b) In the Installation section, double-click Phoenix RSM to download. Be sure to check the version number and operating system.

c) Accept the License Agreement and click the **Start Download** button.

d) Follow installation procedures. Installation guidance can be found either in the Doc folder (after clicking on the downloaded executable), or online at the SoleraTec website, or in the Installation chapter of this guide.

© 2015

## 2. Add a Vault

a) Find your suite of Phoenix RSM applications on your computer (see Launch an Application):

- From a Windows desktop, click **Start** > **All Programs** > **Phoenix**.

- From a Mac desktop, click **Applications** > **Preview**. The Preview window appears. Select **Applications** > **Phoenix** > **Bin**.

- From a Linux desktop, double-click **Filesystem** > **usr** > **local** > **Phoenix** > **Bin**.

b) Open the Add or Remove Vault Wizard and complete the wizard steps to create a Phoenix RSM Vault.

c) Reboot your machine after adding a vault.

All devices running an instance of the product must be **time synchronized**. If they are not, unexpected results may occur.

## 3. Prepare media

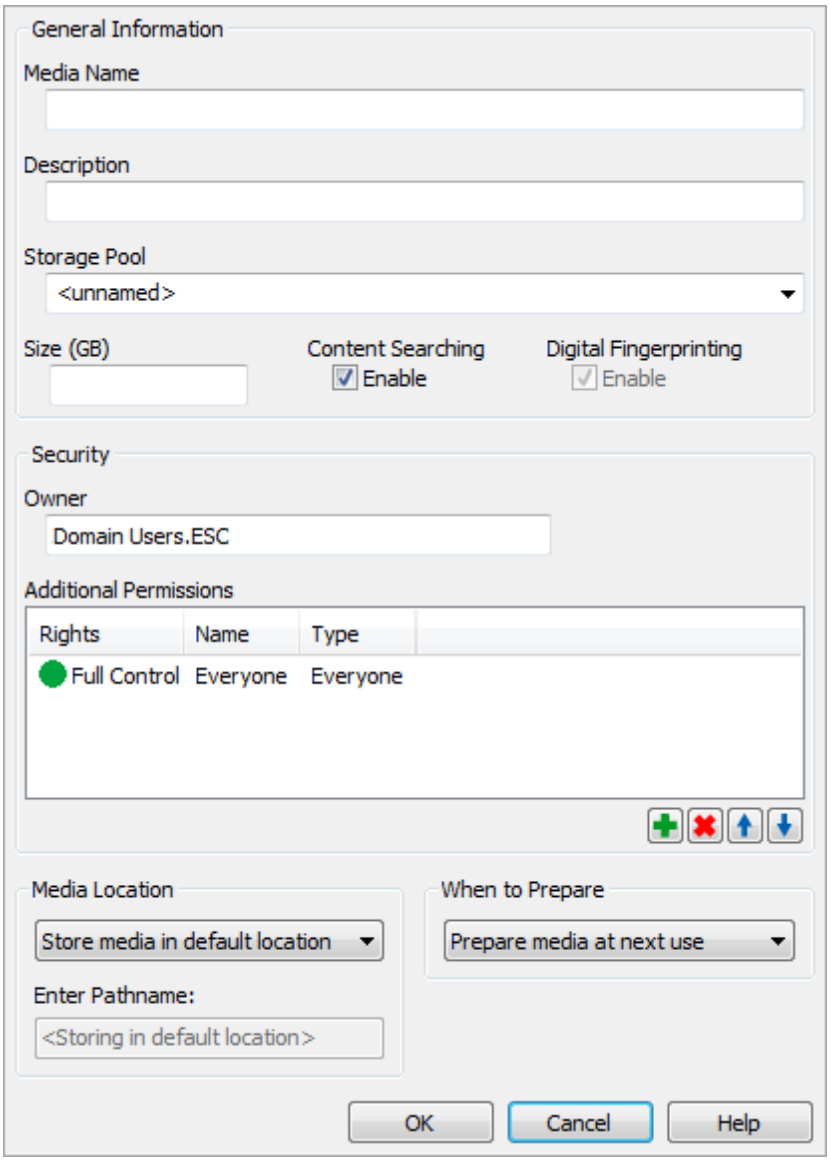
a) From your suite of Phoenix RSM applications, open the Vault Admin application.

b) From the Vault Admin left frame, beneath **Entire Network**, select and expand the items under the Vault you added in the previous step.

c) Select **Media**.

d) For the Prepare Media window, click . The Prepare Media window shown below is for hard disk media; this window is slightly different for other media types.

© 2015




e) In the Prepare Media window, enter a **name** and **description**. For example, the name might be "Camera 1 - Front Lobby" or "Camera 2 - Rear Entrance."

f) In the **Size** (GB) box, type the amount of storage space to make available for the Information Repository. This depends on the total amount of storage capacity of the device and the number of cameras to record video from.

- For example, let's say you have a 1 terabyte (TB) hard drive available for surveillance video storage, and that you are recording from 10 IP cameras.

  1 TB = 1,000 GB

  1,000 GB / 10 cameras = 100 GB for each piece of media.

  You would enter 100.

© 2015

g) Set the **When to Prepare** drop-down list to **Prepare media now**.

h) Click **OK**. The new media appears in the right pane of the Vault Admin window.

i) Click the newly named unit of media, listed beneath the Vault name, in the left pane. Its details appear in the right pane.

j) Repeat the steps above for each unit of media needed.

It is recommended to prepare a separate piece of media for each recording camera.

## 4. Camera setup

### IP Camera users - Connect camera and determine its IP address

a) Refer to the camera's user manual to install, configure, and initially access the camera. The camera needs to be set up with a static IP address or you need to disable DHCP.

b) Use the camera's discovery software or other mechanism to determine its IP address, and write it down. You need it for the next step.

### VMS users - Add camera configuration information

a) From your suite of Phoenix RSM applications, open Camera Policies.

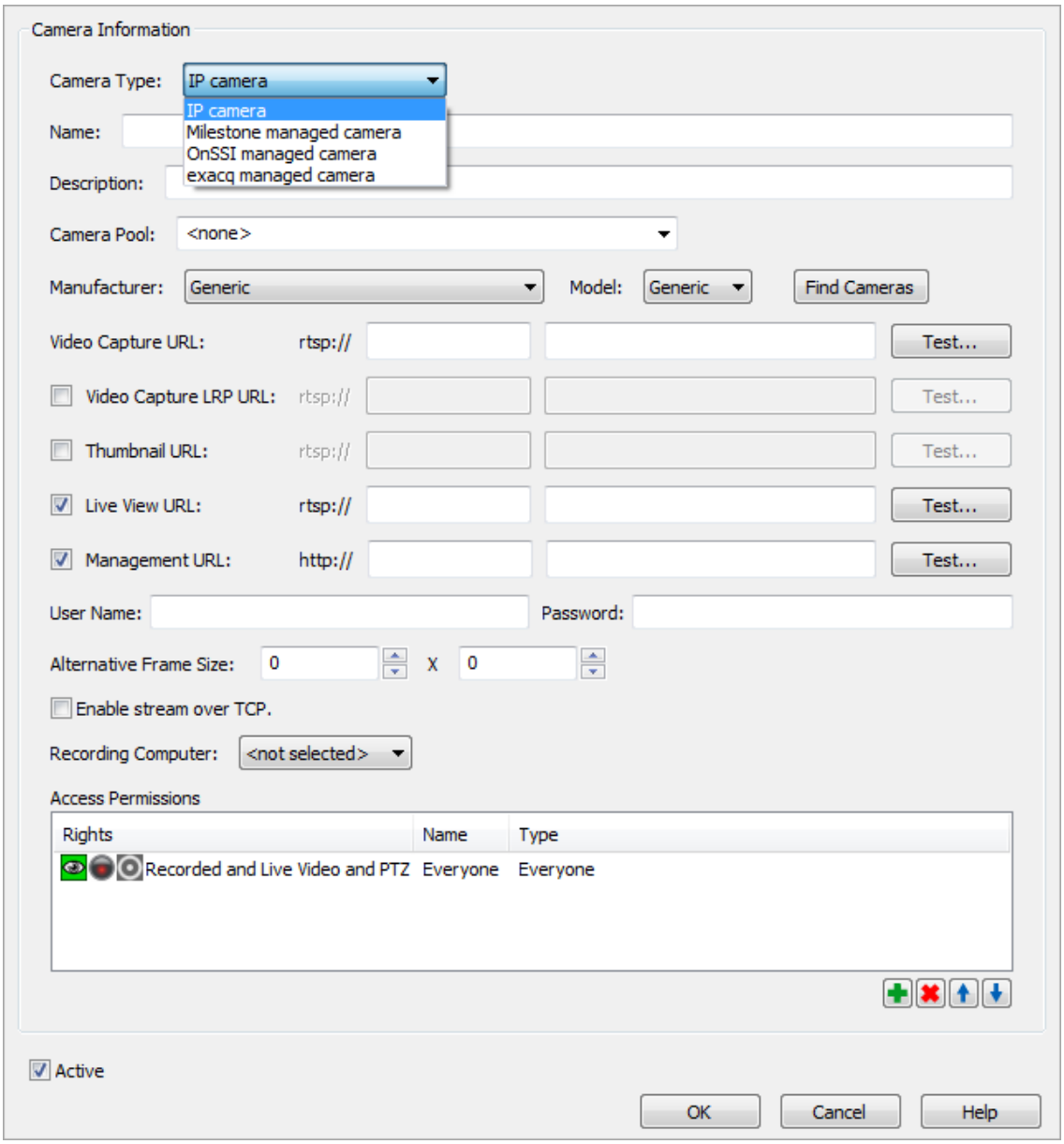
b) From Camera Policies > **View** menu, select **Enable Advanced Mode**.

c) From the toolbar, click the **Cameras** button to open the Camera Configurations window.

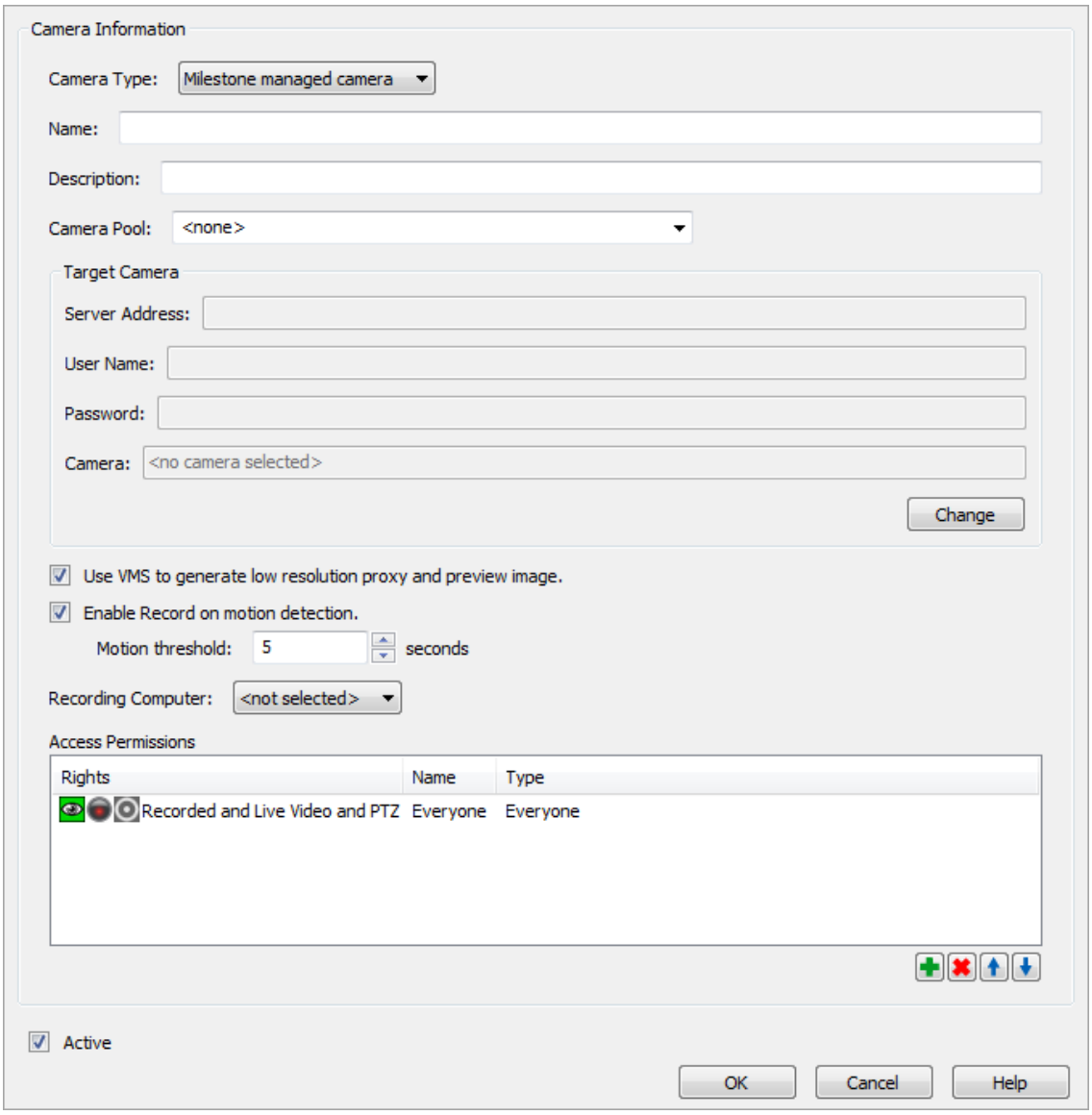
d) From the Camera Configurations window, click the **Add** button to add a new camera configuration.

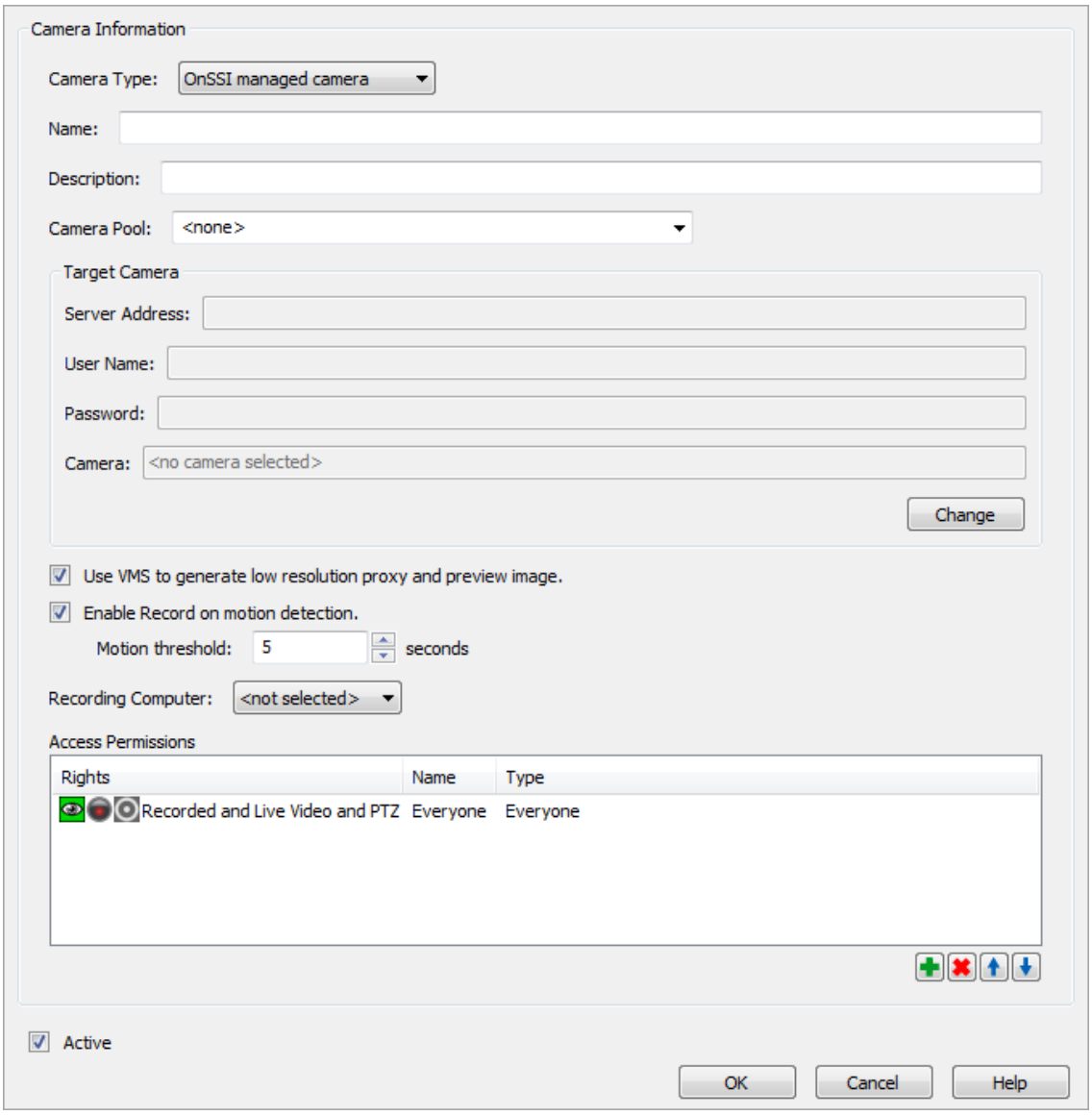
e) From the Camera Type drop-drown list, select a VMS (either **Milestone managed camera**, **OnSSI managed camera**, or **exacq managed camera**).

© 2015

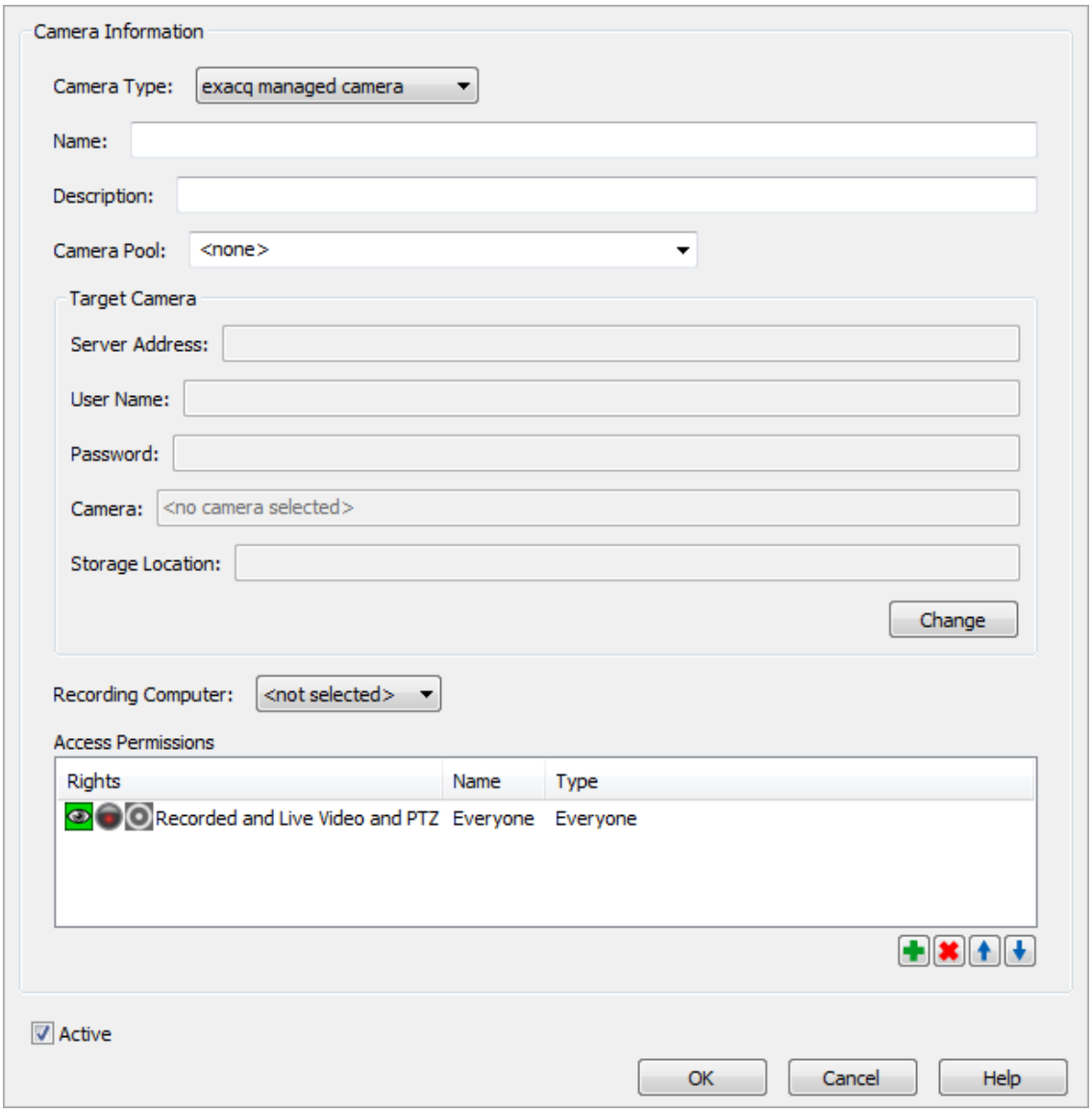

Camera Information
Camera Type:
IP camera
IP camera
Milestone managed camera
OnSSI managed camera
exacq managed camera
Name:
Description:
Camera Pool:
<none>
Manufacturer:
Generic
Model:
Generic
Find Cameras
Video Capture URL:
rtsp://
Test...
Video Capture LRP URL:
rtsp://
Test...
Thumbnail URL:
rtsp://
Test...
Live View URL:
rtsp://
Test...
Management URL:
http://
Test...
User Name:
Password:
Alternative Frame Size:
0
X
0
Enable stream over TCP.
Recording Computer:
<not selected>
Access Permissions
Rights
Name
Type
Recorded and Live Video and PTZ
Everyone
Everyone
Active
OK
Cancel
Help

© 2015


Camera Information
Camera Type:
Milestone managed camera
Name:
Description:
Camera Pool:
<none>
Target Camera
Server Address:
User Name:
Password:
Camera:
<no camera selected>
Change
Use VMS to generate low resolution proxy and preview image.
Enable Record on motion detection.
Motion threshold:
5
seconds
Recording Computer:
<not selected>
Access Permissions
Rights
Name
Type
Recorded and Live Video and PTZ
Everyone
Everyone
Active
OK
Cancel
Help


Camera Information
Camera Type:
OnSSI managed camera
Name:
Description:
Camera Pool:
<none>
Target Camera
Server Address:
User Name:
Password:
Camera:
<no camera selected>
Change
Use VMS to generate low resolution proxy and preview image.
Enable Record on motion detection.
Motion threshold:
5
seconds
Recording Computer:
<not selected>
Access Permissions
Rights
Name
Type
Recorded and Live Video and PTZ
Everyone
Everyone
Active
OK
Cancel
Help

© 2015

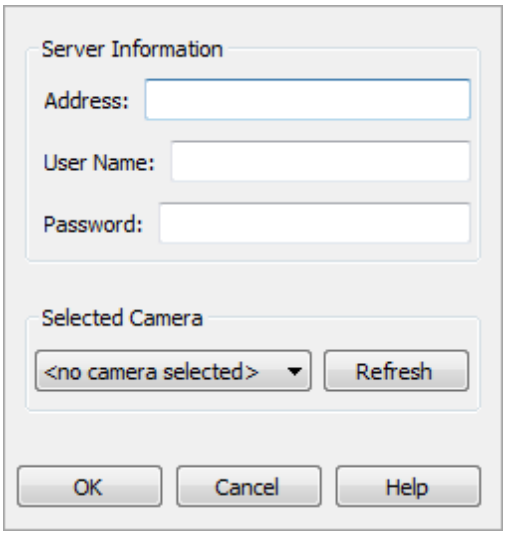


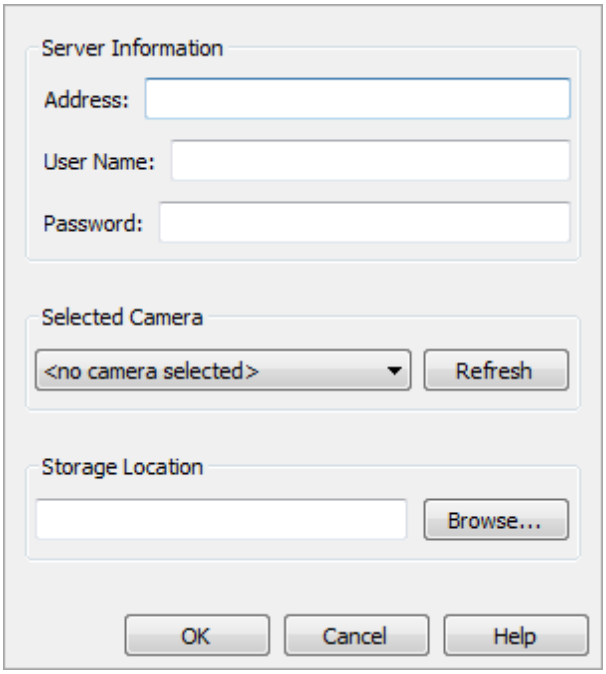

f) Type the **name** and a **description** of the camera.

g) To associate the camera with a **Camera Pool**, select it from the drop-down list. For more information, see Camera Policies.

h) In the **Target Camera** group, click **Change** to populate boxes. The Modify Target dialog box appears.

© 2015




i) Type the **Address**, **User Name**, and **Password**.

j) Click the **Refresh** button to update the list of cameras associated with the server, and then select the camera with video to capture.

k) For Exacq, in the **Storage Location** section, type the path to the video storage area or click **Browse** and navigate to the video storage area.

l) Click **OK** to close the Modify Target dialog box.

m)For Milestone and OnSSI only: In **Video Type**, select the format the extracted video should be stored, either **MJPEG** or **H.264**.

© 2015

n) Leave the **Active** checkbox selected so the camera can be used in the policy to create in the next step.

o) Click **OK** to close the Add New Camera window.

p) Click the Save button to save the new camera configuration and add it to the Information Repository.

q) Repeat the steps above to add the configurations for each camera with video to capture.

For more information see Add VMS Camera.

## 5. Recording setup

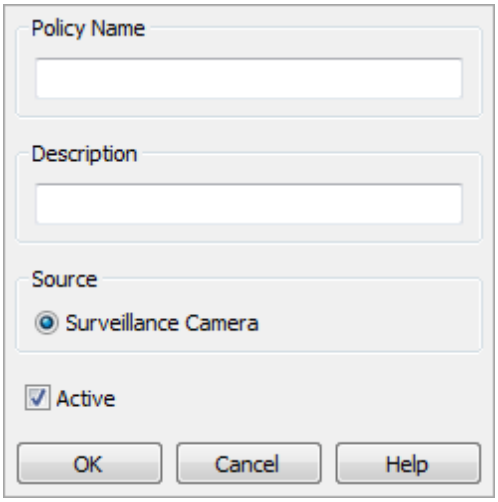
### IP Camera users - Add camera configuration and schedule video recording

Setup for a RTSP-enabled IP camera is very simple. The Phoenix RSM Camera Wizard not only guides you through how to add a RTSP-enabled IP camera, but it also automatically creates a camera (or recording) policy to accompany the camera. The Recording policy designates how to store the recorded video from your camera into the Information Repository.

- See the topic Add Camera Wizard and complete the steps.

### VMS users - Create a recording policy

a) From the Camera Policies application, from the toolbar, click the Add button.




b) In the Create a Policy window, type a **Policy Name** and **Description**, select the **Active** checkbox, and click **OK**.

c) The policy is displayed in the left pane - **Recording Policy Name**, of the Camera Policies window.

d) From the Camera Policies **Camera** tab, select the camera added from the **Camera** drop-down list.

e) In the **Scheduling** tab, leave the defaults so video feeds are recorded continuously.

© 2015

f) Click the **Save** button to save the policy.

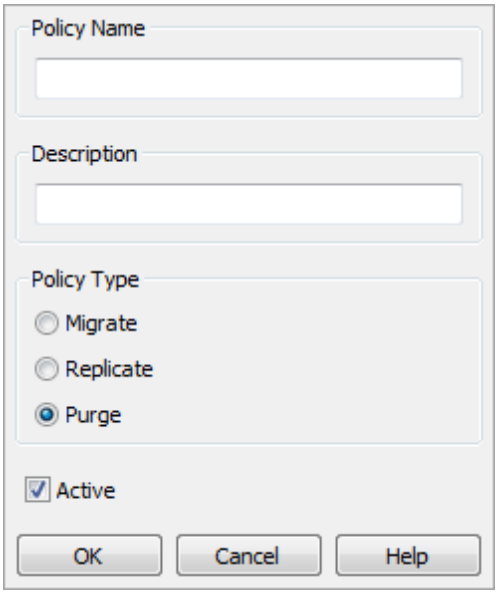
## 6. Create a Data Service policy

It is a good practice to set limits on the amount of space available for video storage. This step sets up that policy so that the oldest video is overwritten before the storage space is full. As limits are reached, new video feeds replace the older ones.

We recommend to set an automatic purge policy; the system ensures each hour that when 80% of the space available has been filled, the oldest clips are overwritten by the new clips being recorded.

a) From your suite of Phoenix RSM applications, open Data Service Policies.

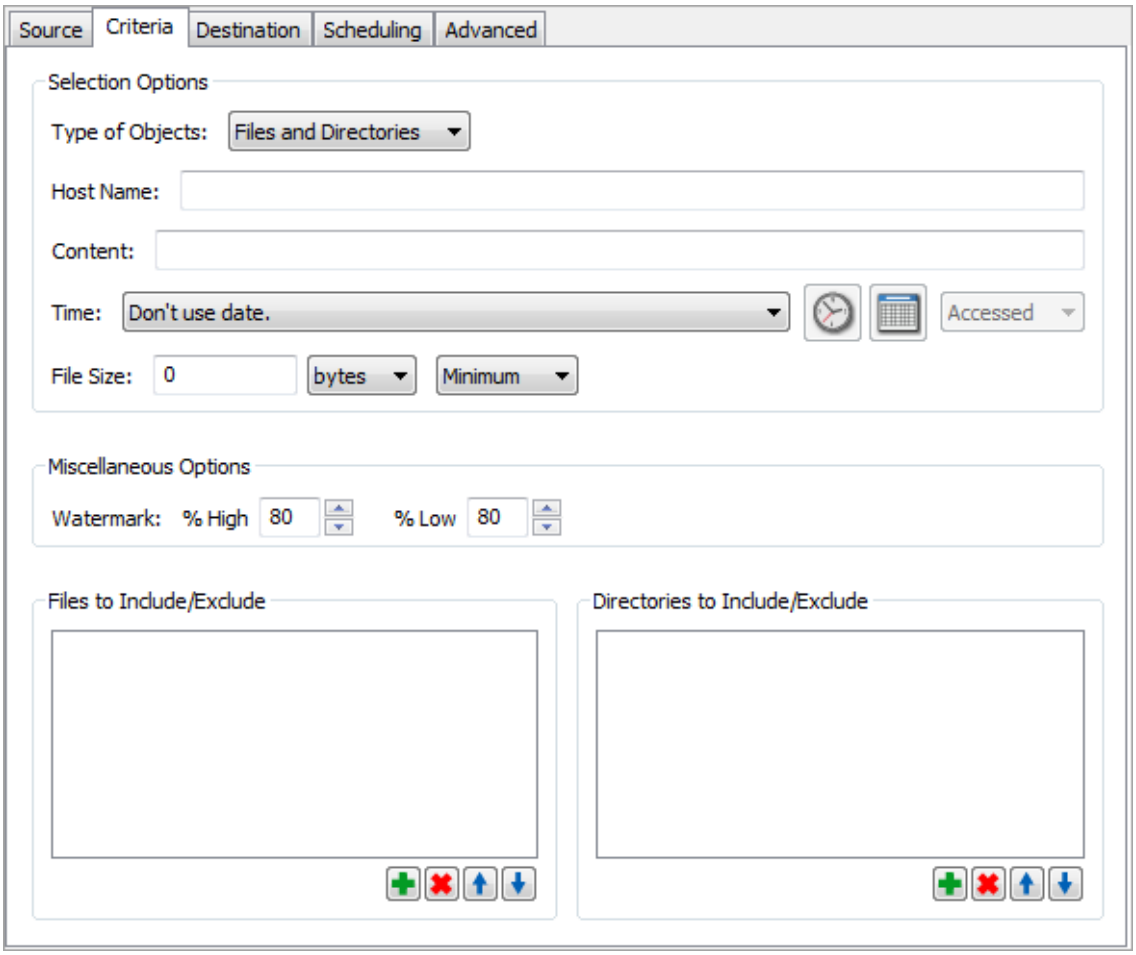
b) From the toolbar of the Data Service Policies window, click the **Add** button .




c) In the Create a Policy window, type a **Policy Name** and **Description**, select a Policy Type of **Purge**, click **Active,** and then click **OK**.

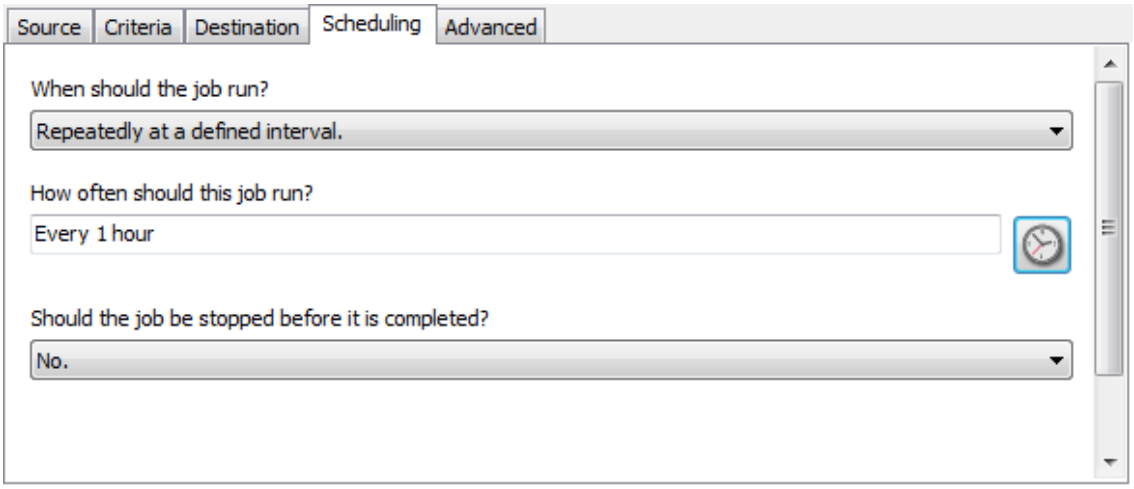
d) From the Data Service Policies window, **Source** tab, leave all the defaults.

© 2015




e) In the **Criteria** tab, under **Miscellaneous Options**, enter **80%** in both the % High and % Low Watermark fields.

f) In the **Destination** tab, none of the boxes are enabled since they are not applicable to a purge type of policy.



g) In the **Scheduling** tab, **When should the job run?** box, select **Repeatedly at a defined interval** .

h) Adjacent to the **How often should this job run?** box, click the Clock button. Type **1** in the **Hours** box, and click **OK**.

i) Click the **Save** button to save the policy.

j) In the **Advanced** tab, leave all the defaults.

## 7. Wait for video feed to record and process

After creating a camera (or recording policy), wait about 15 minutes to allow the system time to record a 5-minute clip, process and store it, and make it available for searching.

## 8. Search for and review recorded video

a) From your suite of Phoenix RSM applications, open Surveillance Video Manager.

b) From the **Search** tab, Search Criteria pane, click the **Search** button. The Search Results pane displays the video clip that was just recorded.

c) From the Search Criteria pane, you could also select the specific camera and search through its video, or click **More Search Options** to see more parameters to narrow search results.

For more information see Search Surveillance Video or Export Surveillance Video to export video out of the system.

## 9. Install Phoenix RSM Client on other computers

To run policies from a computer other than the one where the Vault resides:

**From a CD-ROM**

a) Insert the Phoenix RSM CD-ROM, and open Setup.html.

b) Follow the directions to open the Phoenix RSM Client Bundle, and install the client on the computer.

**To install the software from the SoleraTec website**

a) Go to the SoleraTec website and click the **Download** tab.

b) In the Installation section, double-click Phoenix RSM to download.

c) Accept the License Agreement and click the **Start Download** button.

d) Follow installation procedures. Installation guidance can be found either in the Doc folder (after clicking on the downloaded executable), or online at the SoleraTec website, or in the Installation chapter of this guide.

© 2015

# Vault Management

Vault operation is important to understand as it is key to managing your Information Repository. Vaults can be set up all across your network, which decentralizes your Information Repository for a safe, dynamic, and server-less solution for managing your data assets. Remember that a Vault is a CPU, SoleraTec's Phoenix RSM software, and storage, and each Vault on the network make up your Information Repository. The Vaults themselves have unique licensing and media attributes associated with them.

The tools for managing Vaults on your network are:

- **Add or Remove Vault Wizard** - An application to use for adding or removing a hard disk Vault, standalone data tape Vault, or a data tape library Vault.
- **Vault Admin** - The Vault Admin application allows you to view Vaults on your network. This can be run from the server or from the desktop client component.
- **Vault Services** - Vault Services is the engine that runs a Vault. If there are multiple Vaults, then a Vault Service runs for each Vault. This service must be run on the server component.

There are several facets to Vault management, most having to do with preparing and managing media. The Vault Admin is designed to support the day-to-day tasks associated with managing Vaults. For more information see Vault Admin.

## Basic Media Concepts

Phoenix RSM Vaults use media to store video and data, all of which is protected and managed by the Information Repository. By using the Vault Admin application, you can manage media in your Information Repository.

Managed media can be in a physical form, such as a digital computer data tape, or it can be in a virtual form, such as a portion of hard disk assigned for use by the Information Repository. The list of media utilized is constantly being expanded, and every type of media has features that make it suitable for a certain purpose. For example, hard disk is a good medium to process files to because there is no latency associated with it. It is ready to accept data as it is sent from network clients and it can service several clients at the same time.

The media hierarchy is organized as such:

- The highest level of the hierarchy is the Vault itself.
- Media units are the next level and they coincide with logical media units like data tapes or portions of hard disks.
- The volume level is lowest. Volumes are sections of media units. They can be as large as the media itself or very small.

On some media, there can be one or several volumes on a unit. There can be one or more units of media in a Vault. There can also be multiple Vaults on a single host computer, depending on its performance and storage pools - where one or more pieces of media are linked together for a common use.

All managed media is configured with common elements including: label, header, data storage area, on-media catalog, data tape media, hard disk media, and virtual media.

© 2015

### Media Retention and Purging

Administrators can eliminate outdated data on supported media.

For hard disk Vaults, use Data Service Policies to define file retention rules for removing duplicated data or for retaining source data indefinitely. The same retention rules can be used even if files are never copied or moved. This allows data to be erased after a pre-defined period.

Using Vault Admin, you can erase media which overwrites erased files. When you erase data tape media, there is a delay in the actual event until just before the media is re-used. This ensures easy management of many units of media without having to wait for long delays associated with loading and positioning of media. If you do not want a delay, you can override the delay and execute the erase immediately.

### Workflow - Basic Vault Steps

1. From your suite of product applications, open the Add or Remove Vault Wizard application (AddRemVltWzrd.exe). For further explanation of how to launch applications using different operating systems, see Getting Started.
2. You'll need to add a Vault before you do anything. Once added, it is up and running automatically.
3. Media is used to store your files or video. Designate your media type and a place to which to store your media. See Prepare Media.
4. After your media is prepared, then you'll need to load your media. See Load Media.
5. Vault parameters can be viewed and edited through the Vault Properties. Or, Vault activity can be monitored using Network Activity.
6. Vaults can be removed or shut down at any time. See Remove Vaults and Vault Shutdown or Restart.

## Add Vaults

After your Phoenix RSM clients are installed and configured, add Vaults using the Add or Remove Vault Wizard. Use the Add or Remove Vault Wizard before or in conjunction with the Vault Admin, but in order to administrate a Vault, a Vault must be added first. (When removing Vaults use the same wizard, see Remove Vaults.)

Keep the following in mind:

- You must have administrative rights to add a Vault.
- All devices running in Phoenix RSM must be time synchronized. If they are not, unexpected results may occur.
- To change Vault settings, including the naming of Vaults, security, logs, notifications, diagnostics, memory allocation for devices, database optimization parameters, and licensing after you have installed a Vault, see Vault Properties.

© 2015

## Vault Considerations

Vaults are installed on computers to control and manage storage devices. The computer hosting a Vault needs adequate resources to operate and manage the storage device, and considerations should be made for growth and scale. As the amount of data being stored increases, the volume of entries in the Vault database also increases. Vaults that use high capacity storage devices need system resources to accommodate.

| Consideration | Description |
|---|---|
| **Calculating Needed Memory for the Vault Catalog** | The Vault database requires about 2% of the total amount of available storage space. |
| **Date and Time Properties on Computers with Vaults** | All computers that contain Vaults and any VMS system that video is captured from must be synchronized to the same time source for the Information Repository to function correctly. |
| **Hosting More than a Single Vault on One Computer** | A single computer can host up to four Vaults as long as it is equipped with enough processor power, memory, and disk space to accommodate the needs of the storage Vaults. This type of configuration is common in smaller environments where a disk-based and a tape-based Vault are both configured on a single computer.<br> Configure multiple Vaults on a single network computer, but for optimal performance it is recommended that Vaults reside on computers other than those where Camera policies and the Surveillance Video Manager are implemented. |
| **Starting or Restarting Vaults Manually** | If added Vaults are not visible by the Information Repository, you may have to start them manually. See Start Vaults Manually. |
| **Security/Rights** | When adding a Vault, it is accessible to all users. To change Vault rights see Vault Properties Security tab. |

## Workflow - Add Vaults

Work through the following steps to add Vaults to your Information Repository:

1. Add Vaults using the wizard.
2. Reboot the computer with added Vaults.
3. Prepare media using Vault Admin.

© 2015

## Add or Remove Vault Wizard

Use the Phoenix RSM Add or Remove Vault Wizard to add or remove a hard disk Vault, shadow hard disk Vault, standalone tape Vault, or tape library Vault. Unless you are an advanced user and have clearly defined reasons for changing the default values, it is best to use default values, leaving **advanced user mode** de-selected. Most settings can be modified after the fact using Vault Properties. After adding a Vault, the next step is to prepare media for your Vault and Information Repository.

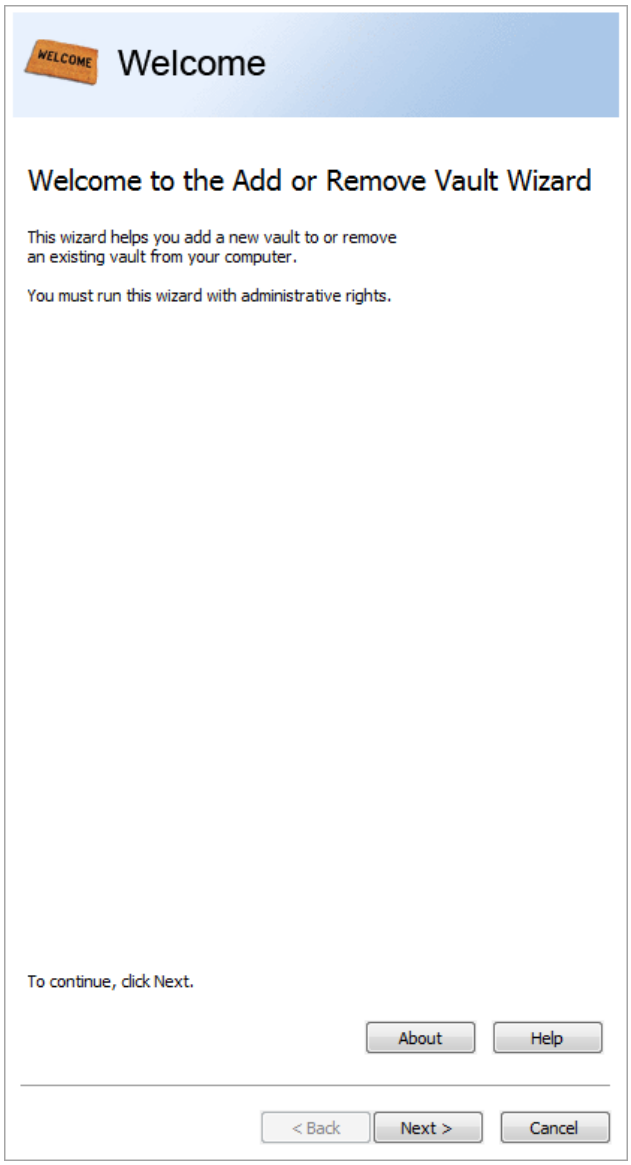
If running the wizard in standard mode, not all of the wizard windows appear for you because the wizard uses default values for setup. The screenshots below have advanced mode selected so you can see all wizard windows.

### Adding a Vault

1. From your suite of product applications, open the Add or Remove Vault Wizard application (AddRemVltWzrd.exe). The Welcome window appears. Each wizard dialog box includes **Back**, **Next** , **Help**, and **Cancel** buttons. The **Back** button navigates you back to the previous dialog box (except on the Welcome window), and the **Next** button accepts current values and advances you to the next window in the wizard. The **Help** button opens documentation, and the **Cancel** button closes the wizard without saving values.

The **About** button appears on the first wizard window to provide information, and the **Finish** button appears on the last wizard window to complete the process.

© 2015

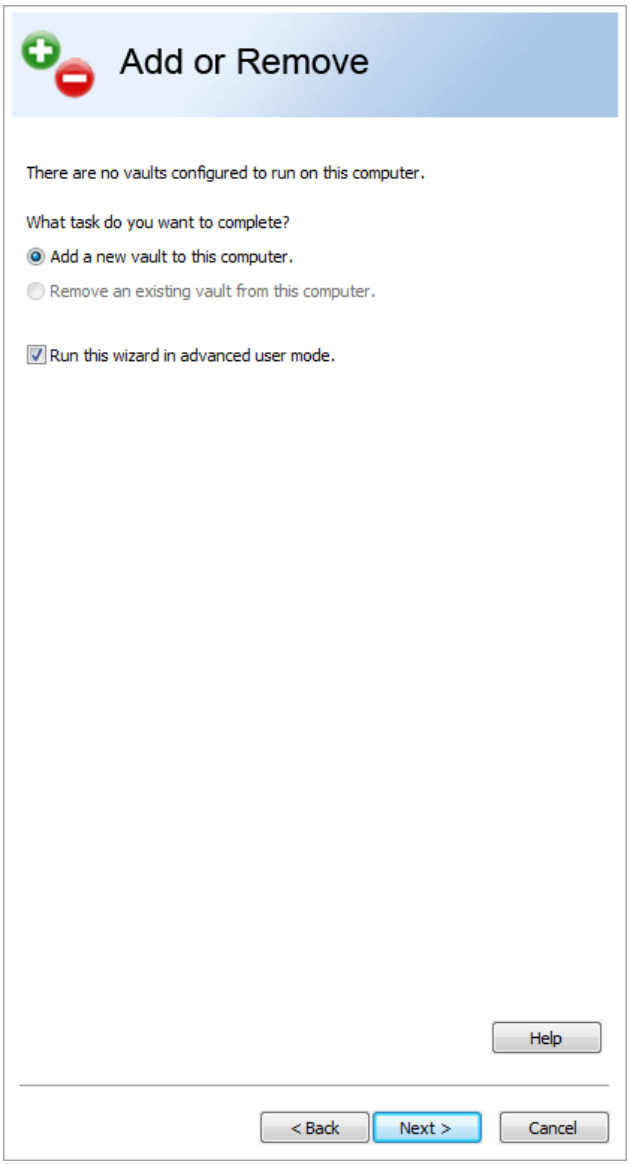

Welcome
Welcome to the Add or Remove Vault Wizard
This wizard helps you add a new vault to or remove an existing vault from your computer.
You must run this wizard with administrative rights.
To continue, click Next.
About
Help
< Back
Next >
Cancel

2. Click **Next** for the Add or Remove window

   - Select either **Add a new Vault to this computer** or **Remove an existing Vault from this computer**. Depending on your selection the wizard follows the path for you to add a Vault or to remove one. If removing a Vault, see Remove Vaults.
   - Select **Run this wizard in advanced mode** to bypass default values and customize Vault parameters. These instructions cover all of the advanced mode options but it is recommended to run in standard mode, leaving this option de-selected.

   If there are four Vaults installed on the computer where the wizard is run from, then **Add new Vault to this computer** is disabled. In that case, delete a Vault before adding a new one.

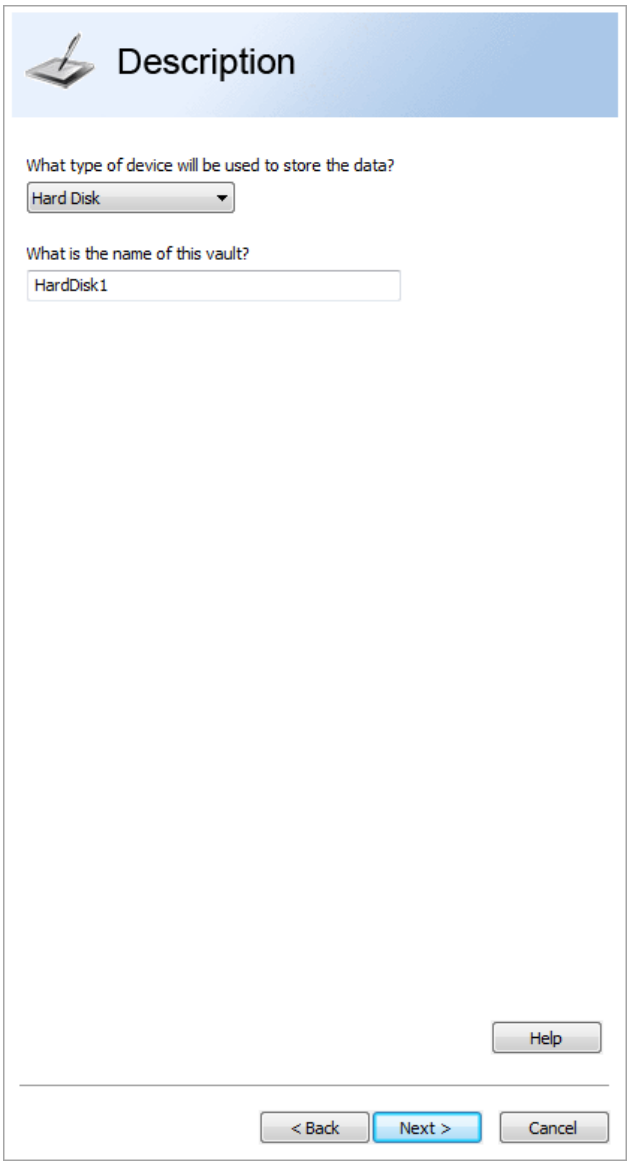
© 2015


Add or Remove
There are no vaults configured to run on this computer.
What task do you want to complete?
Add a new vault to this computer.
Remove an existing vault from this computer.
Run this wizard in advanced user mode.
Help
< Back
Next >
Cancel

3. Click **Next** for the Description window.

- From the **What type of device will be used to store the data?** drop-down list, select either Hard Disk, Tape Library, Stand Alone Tape Drive, or Veracity Coldstore. Depending on your selection, subsequent content on wizard windows change accordingly.
- In the **What is the name of this Vault**, type a Vault name or use the default if it is already populated with a name you want to use.

© 2015




4. Click **Next** for the Device window (appears for advanced mode only). The **Device** window enables you to define how many data streams are allowed simultaneously and how many files are kept in a directory. To work through the Device window for your storage device type, see the appropriate heading below:

Hard Disk

- From the **How many data streams are allowed at a time?** drop-down list, select from a range of 1 - 10. Data streams refers to the number of connections made to a Vault at once. Several connections enables clients to communicate with the Vault simultaneously. The more streams permitted requires more processing power.

© 2015

- From the **How much memory should be used for each data stream cache?** drop-down list, select between 5, 10, 15, or 20 MB. Here, you are defining how much virtual memory is set aside for incoming and outgoing data during file storage and retrieval. A larger cache can improve performance, but at the expense of using more virtual memory. The total amount of space used equals the number of data streams multiplied by the selected cache size. With 10 data streams and 10 MB of cache, the Vault sets aside 100 MB of total virtual memory for caching data. A selection of 10 MB is usually sufficient.

- From the **When storing data, how many files will be kept in a directory?** drop-down list, select between 50 - 500. Data is stored in files in the Vault. More files provides more storage on the media, but also slows down performance. The following details the number of files that correlates with each value.

| Value | Number of Files |
|---|---|
| 50 | 125 billion |
| 100 | 250 billion |
| 150 | 375 billion |
| 200 | 500 billion |
| 300 | 750 billion |
| 400 | 1 trillion |
| 500 | 125 trillion |

- In the **Where will media be stored by default?** box, type a default location to store and manage media, or select a default location from the Browse for Folder window by clicking the **Browse** button.

- From the **Do you want storage media to be created automatically?** drop-down list, choose **Yes** or **No**.

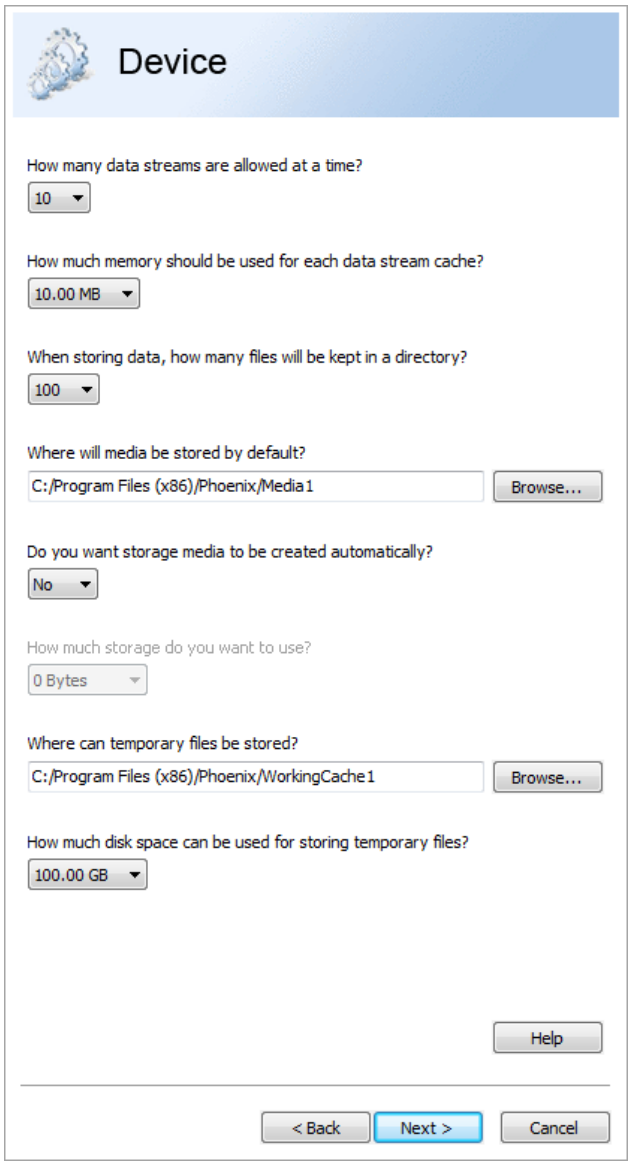
    - If you choose Yes, from the **How much storage do you want to use?** drop-down list, choose a value between 0 Bytes and 10.00 TB. Media will automatically be created for your Vault.

    - If you choose No, media will need to be created manually at a later time. See Prepare Media.

- From the **Where can temporary files be stored?** box, type a location for the working cache, or select a location from the Browse for Folder window by clicking the **Browse** button. The default location is <install-dir>/WorkingCache. When Phoenix RSM processes files, it may create temporary files for efficient performance; especially when clipping video files.

- From the **How much disk space can be used for storing temporary files?** drop-down list, select how much working cache space is used for temporary files.

© 2015


Device
How many data streams are allowed at a time?
10
How much memory should be used for each data stream cache?
10.00 MB
When storing data, how many files will be kept in a directory?
100
Where will media be stored by default?
C:/Program Files (x86)/Phoenix/Media1
Browse...
Do you want storage media to be created automatically?
No
How much storage do you want to use?
0 Bytes
Where can temporary files be stored?
C:/Program Files (x86)/Phoenix/WorkingCache1
Browse...
How much disk space can be used for storing temporary files?
100.00 GB
Help
< Back
Next >
Cancel

Tape Library

If you are using Windows Vista or older, or Windows Server 2008 or older, you must first disable the tape library and tape drives in the Windows Device Manager so Windows does not interfere with Phoenix RSM's management of the device. See Disable SCSI Devices.

- From the **Which tape library do you want to use?** box, select a device. If no devices are found, make sure the tape drive is connected to your computer and powered on. If you are adding a Vault to a Windows computer, ensure that the device or devices are disabled in the Windows Device Manager. Then, click **Look for Devices** to refresh the list.

© 2015

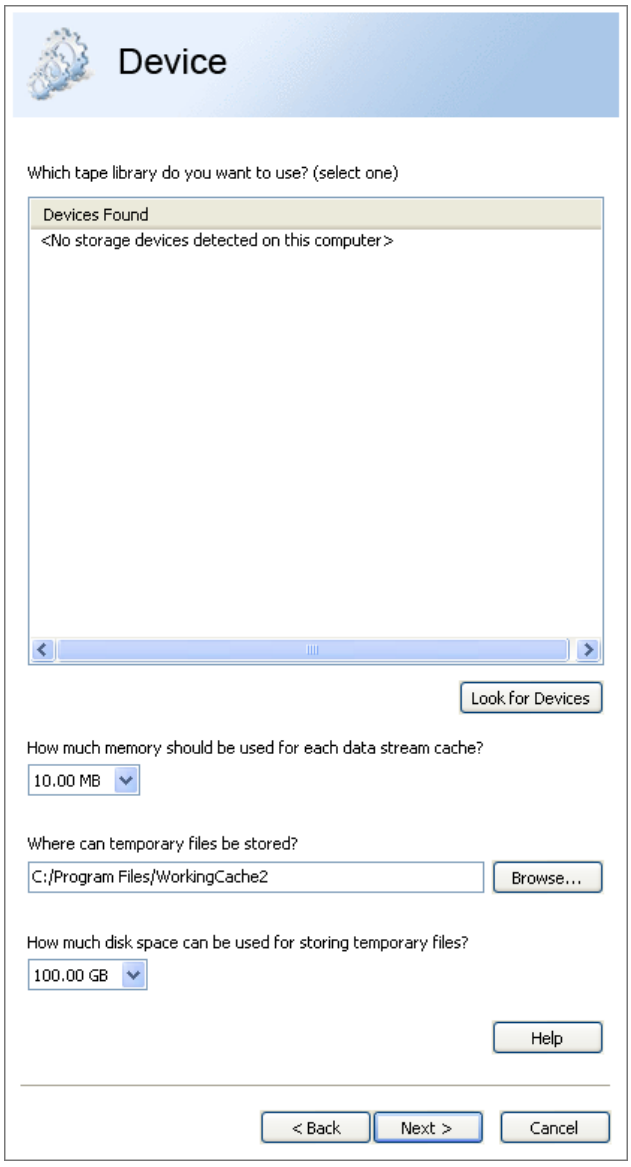
- Some tape libraries do not support automatic detection of their tape drives. The phrase **drives need to be identified** appears to the right of the device name. When **Next** is clicked, you need to select the drives.

- From the **How much memory should be used for each data stream cache?** drop-down list, select between 5, 10, 15, or 20 MB. Define how much virtual memory is set aside for incoming and outgoing data during file storage and retrieval. A larger cache can improve performance, but at the expense of using more virtual memory. The total amount of space used equals the number of data streams multiplied by the selected cache size. With 10 data streams and 10 MB of cache, the Vault sets aside 100 MB of total virtual memory for caching data. A selection of 10 MB is usually enough.

- From the **Where can temporary files be stored?** box, type a location for the working cache, or select a location from the Browse for Folder window by clicking the **Browse** button. The default location is <install-dir>/WorkingCache. When Phoenix RSM processes files, it may create temporary files for efficient performance; especially when clipping video files.

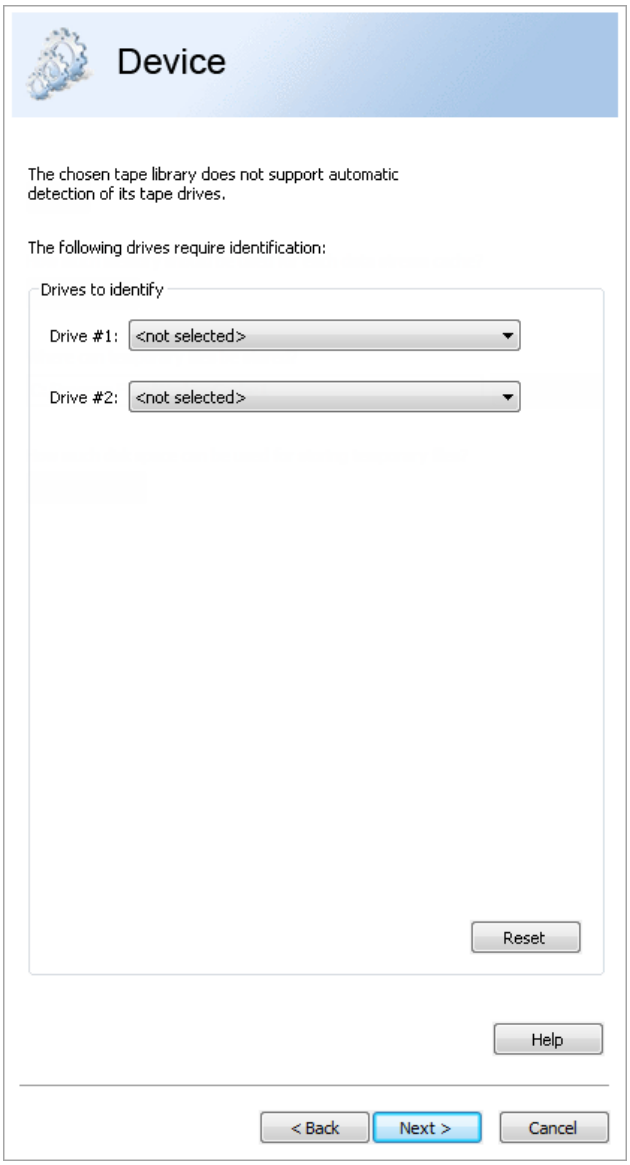
- From the **How much disk space can be used for storing temporary files?** drop-down list, select how much working cache space is used for temporary files. The working cache should be large enough to hold multiple large video files. The default size is 100 GB.

*© 2015*




- Click **Next**. If the tape library was not able to provide the identification for its tape drives, a second device window appears. From the **Drives to identify** group drop-down lists, select the drives. If the device was able to identify its tape drive, then the next wizard window appears.

© 2015




Standalone Tape Drive Vault

If you are using Windows Vista or older, or Windows Server 2008 or older, you must first disable the device in the Windows Device Manager so Windows does not interfere with Phoenix RSM's management of the device. See Disable SCSI Devices.

- From the **Which standalone tape drive do you want to use?** box, select a device. If no devices are found, make sure the tape drive is connected to your computer and powered on. If you are adding a Vault to a Windows computer, ensure that the device or devices are disabled in the Windows Device Manager. Then, click **Look for Devices** to refresh the list.

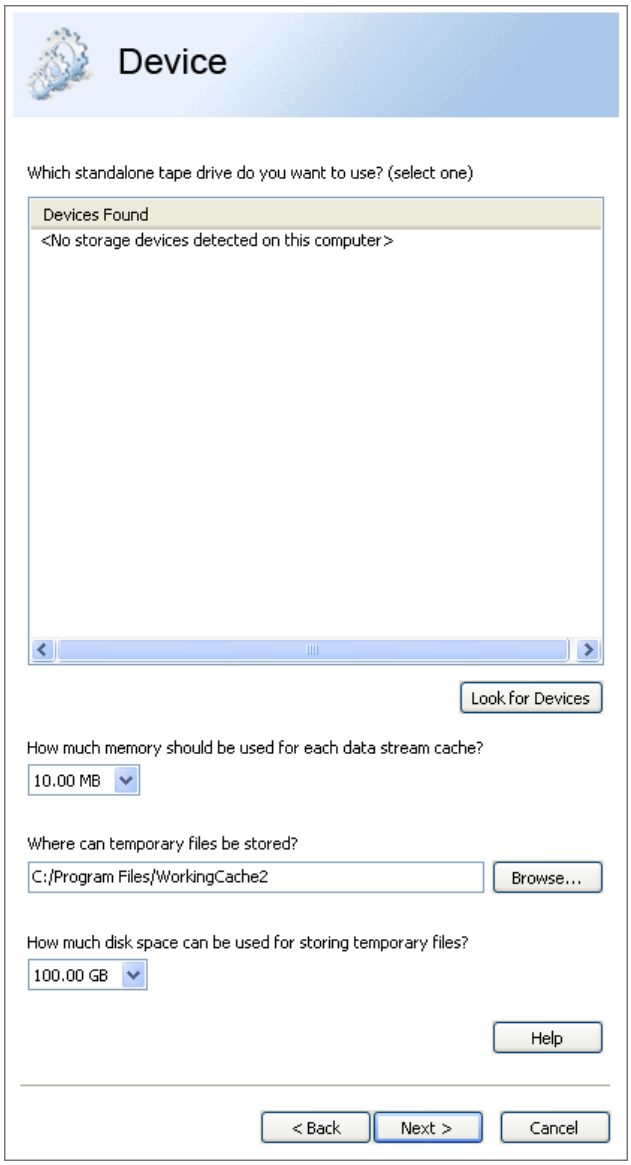
© 2015

- From the **How much memory should be used for each data stream cache?** drop-down list, select between 5, 10, 15, or 20 MB. Define how much virtual memory is set aside for incoming and outgoing data during file storage and retrieval. A larger cache can improve performance, but at the expense of using more virtual memory. The total amount of space used equals the number of data streams multiplied by the selected cache size. With 10 data streams and 10 MB of cache, the Vault sets aside 100 MB of total virtual memory for caching data. A selection of 10 MB is usually enough.

- From the **Where can temporary files be stored?** box, type a location for the working cache, or select a location from the Browse for Folder window by clicking the **Browse** button. The default location is <install-dir>/WorkingCache. When Phoenix RSM processes files, it may create temporary files for efficient performance; especially when clipping video files.

- From the **How much disk space can be used for storing temporary files?** drop-down list, select how much working cache space is used for temporary files. The working cache should be large enough to hold multiple large video files. The default size is 100 GB.

© 2015




Veracity Coldstore

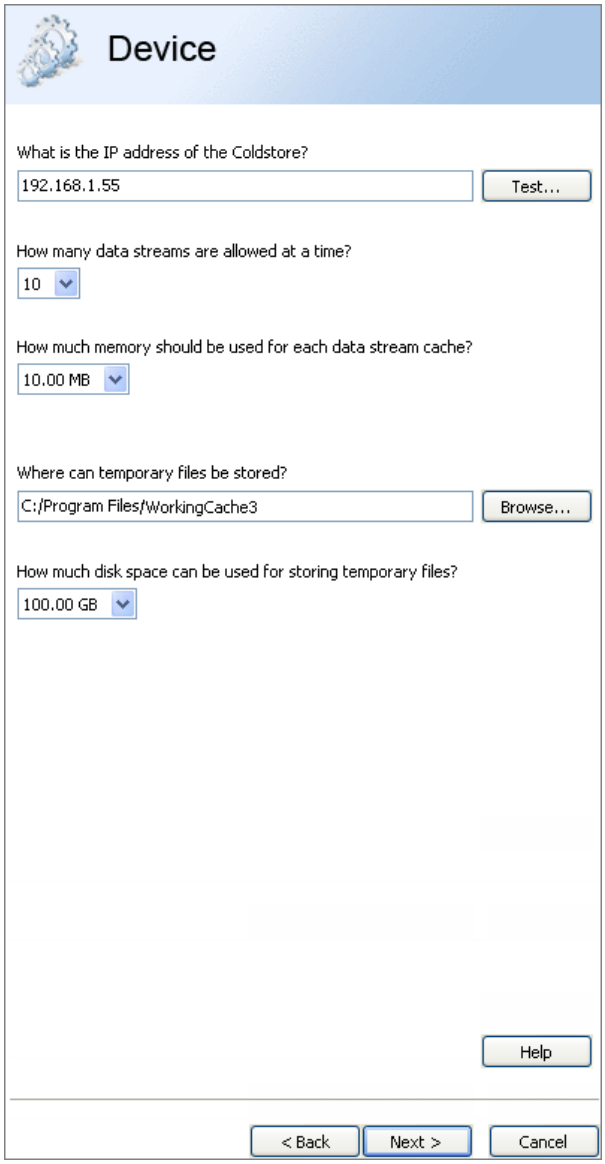
- In the **What is the IP address of the Coldstore?** text box, the IP address of the Veracity Coldstore device. The IP address must be in dot notation. Click the **Test** button to test connectivity to the device.
- From the **How many data streams are allowed at a time?** drop-down list, select from a range of 1 - 10. Data streams refers to the number of connections made to a Vault at once. Several connections enables clients to communicate with the Vault simultaneously. The more streams permitted requires more processing power.

© 2015

- From the **How much memory should be used for each data stream cache?** drop-down list, select between 5, 10, 15, or 20 MB. Here, you are defining how much virtual memory is set aside for incoming and outgoing data during file storage and retrieval. A larger cache can improve performance, but at the expense of using more virtual memory. The total amount of space used equals the number of data streams multiplied by the selected cache size. With 10 data streams and 10 MB of cache, the Vault sets aside 100 MB of total virtual memory for caching data. A selection of 10 MB is usually sufficient.

- From the **Where can temporary files be stored?** box, type a location for the working cache, or select a location from the Browse for Folder window by clicking the **Browse** button. The default location is <install-dir>/WorkingCache. When Phoenix RSM processes files, it may create temporary files for efficient performance; especially when clipping video files.

- From the **How much disk space can be used for storing temporary files?** drop-down list, select how much working cache space is used for temporary files.

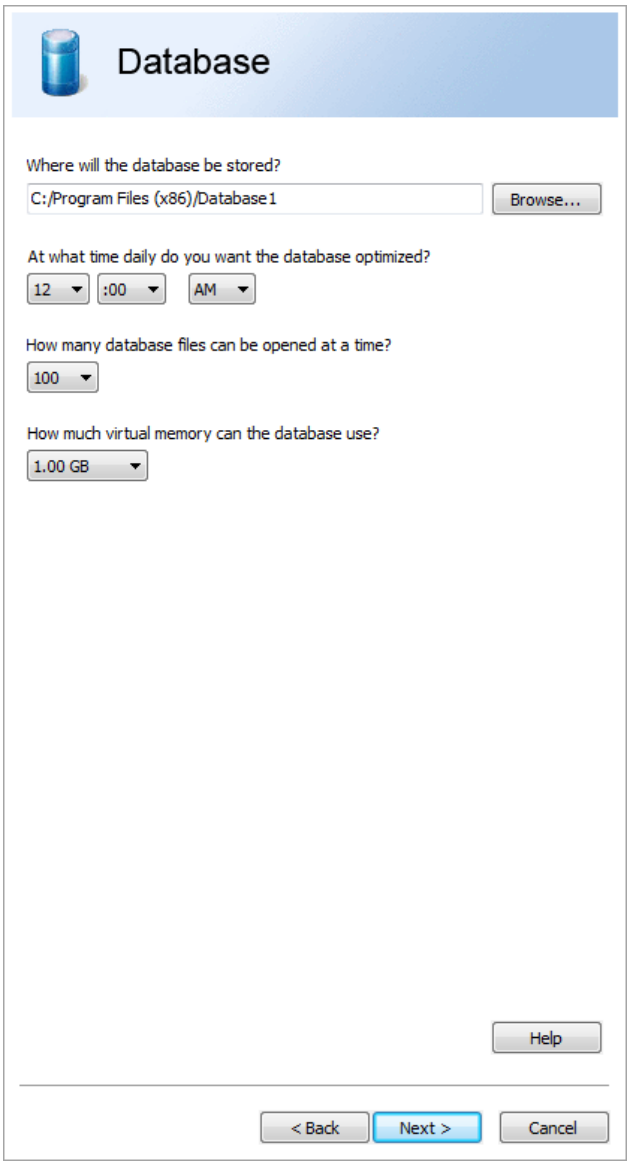



© 2015

5. Click **Next** for the Database window (appears for advanced mode only). The database keeps track of Vault contents, information, and metadata.

    - From the **Where will the database be stored?** box, type the location to store the database, or select a location from the Browse for Folder window by clicking the **Browse** button.
    - Using the **At what time daily do you want the database optimized?** drop-down lists, set the hours, minutes, and AM/PM for how often the database gets optimized to make sure Phoenix RSM and the Information Repository continue to function optimally.
    - From the **How many database files can be opened at a time?** drop-down list, select between 10 - 500 to limit how many files can be open at once. Having more files open allows for a faster search, but more files requires more Information Repository resources.
    - From the **How much virtual memory can the database use?** drop-down list, select between 256 MB - 2 GB. For best Information Repository performance, select a value that does not exceed 75% of the physical memory on the computer.

*© 2015*



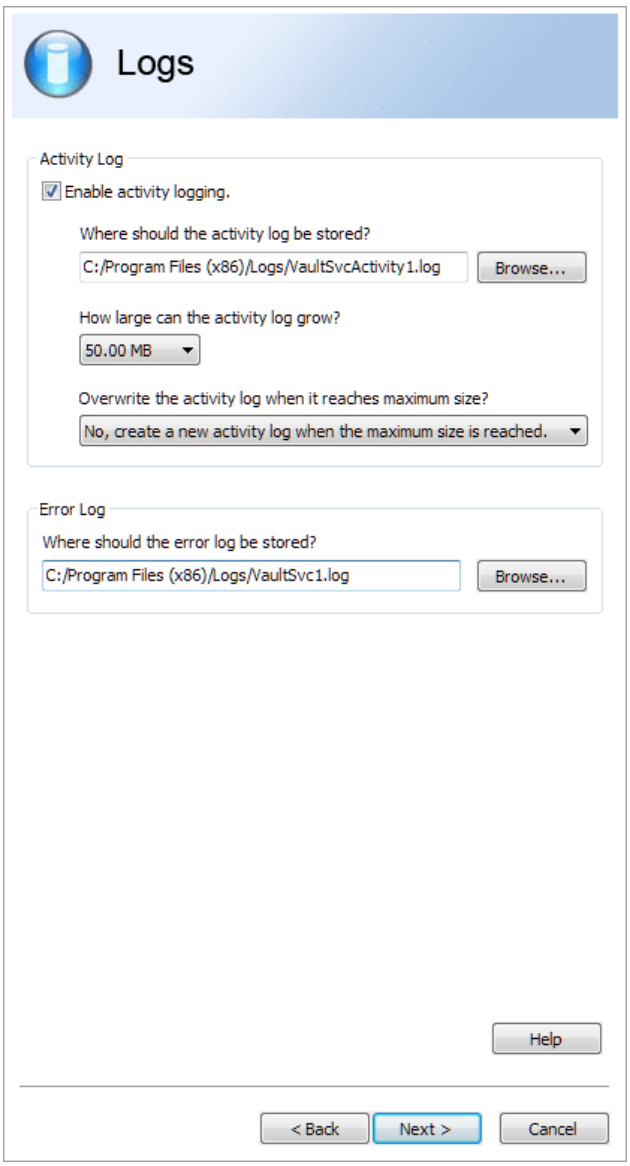

6. Click **Next** for the Logs window (appears for advanced mode only). Use to define where activity and error logs are written to.

   - Select **Enable activity logging** to activate logging functionality. Activity logs provide a security audit trail for these events: Vault start, Vault stop, file read, file write, file create, file delete, media load, media unload, and media erase. For these events, the name and IP of the user who executed the event and the date and time the event was executed are reported. Activity logging is optional, but if activated they create in a tab-delimited format and can be viewed in any application that supports the format, such as Microsoft Excel.

   - From the **Where should the activity log be stored?** box, type a location of where to write activity logs, or select a location from the Activity Log Location dialog box by clicking the **Browse** button.

© 2015

- From the **How large can the activity log grow?** drop-down list, select between 25.00 MB - 1.00 GB to define the maximum size an activity log can grow to. Limit the size of the log because it can be difficult to find specific information in a huge activity log.
- From the **Overwrite the activity log when it reaches maximum size?** drop-down list, select either **Yes** or **No**. By selecting No, a new activity log is created whenever the current activity log reaches the maximum size. Overwriting the activity log prevents against proliferation.
- From the **Where should the error log be stored?** box, type a location of where to store error logs, or select a location from the Error Log Location dialog box by clicking the **Browse** button. Error logs are always enabled and are created when a Vault encounters a problem. Error logging is supported for every Vault in your Information Repository; the logs include warning and Vault start and stop information.



7. Click **Next** for the Notification window. Use to define where e-mails about Information Repository events are sent and where Phoenix RSM events should be logged.

   - Select the **Enable e-mail notifications** checkbox to receive an e-mail when an event occurs of interest for managing a Vault. The events include Vault start, Vault stop, media requests, etc., and are the same as those recorded for notifications. If de-selected, no notifications are sent and other fields in the group box are disabled.

   - In the **Who should receive e-mail notifications?** box, type the e-mail address of the user receiving the Phoenix RSM event notifications.

   - In the **What is the name or IP address of your mail server?** box, type the address of your mail server. Use either IP address or computer name, and then click the **Send Test Email** to test the path. If successful, a dialog box displays, "A message had been sent and should be delivered shortly". Click **OK** to close the dialog box. Valid parameters are not tested here. If parameters are invalid, then the e-mail notifications do not work.

   - From the **Where should events be logged?** drop-down list, select one of the following for where events are logged:

     **Computer Console** - Events are logged in a computer monitor console. It remains open as long as the Vault is running. If the Vault is stopped, the console disappears. If the Vault is restarted, the console disappears and then reappears.

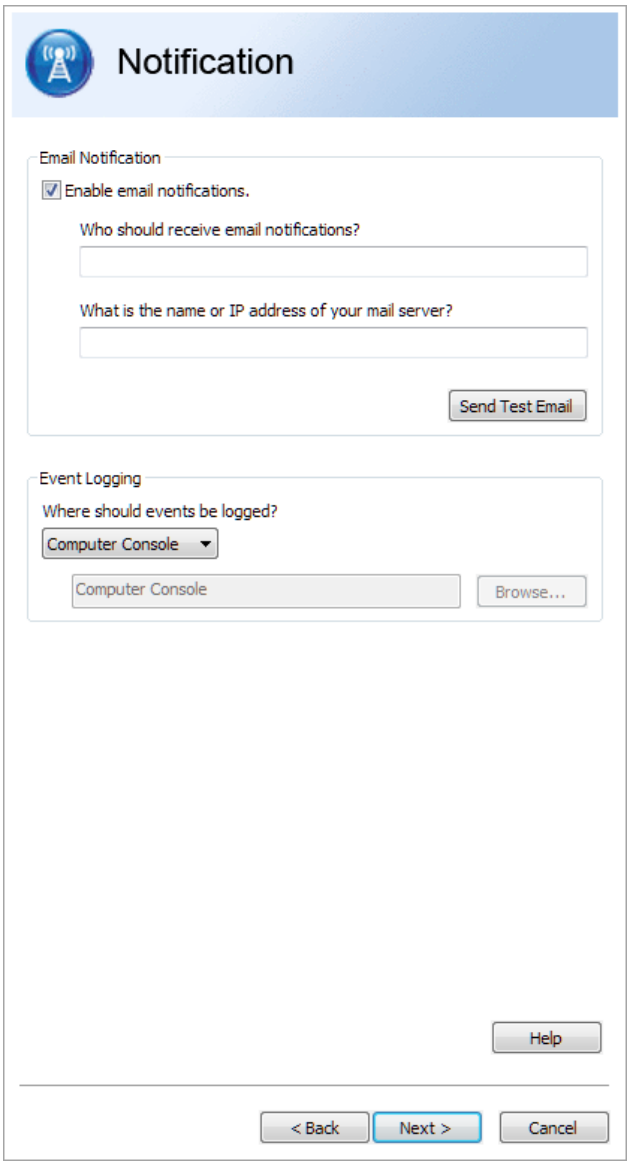
     **Window** - Events are logged in computer monitor window. It remains open as long as the Vault is running. If the Vault is stopped, the window disappears. If the Vault is restarted, the window disappears and then reappears.

     By selecting **Computer Console** or **Window** in a Windows environment, configure Vault service on Windows to open a window on the desktop for diagnostic messages. Once configured, Vault activity displays.

     If you close a window or console, the Vault stops. Phoenix RSM does not operate without running Vaults.

     **File** - Events are logged to a file. With this option, type the file name to store the events, or select a location from the Event Log Pathname dialog box by clicking the **Browse** button.

© 2015

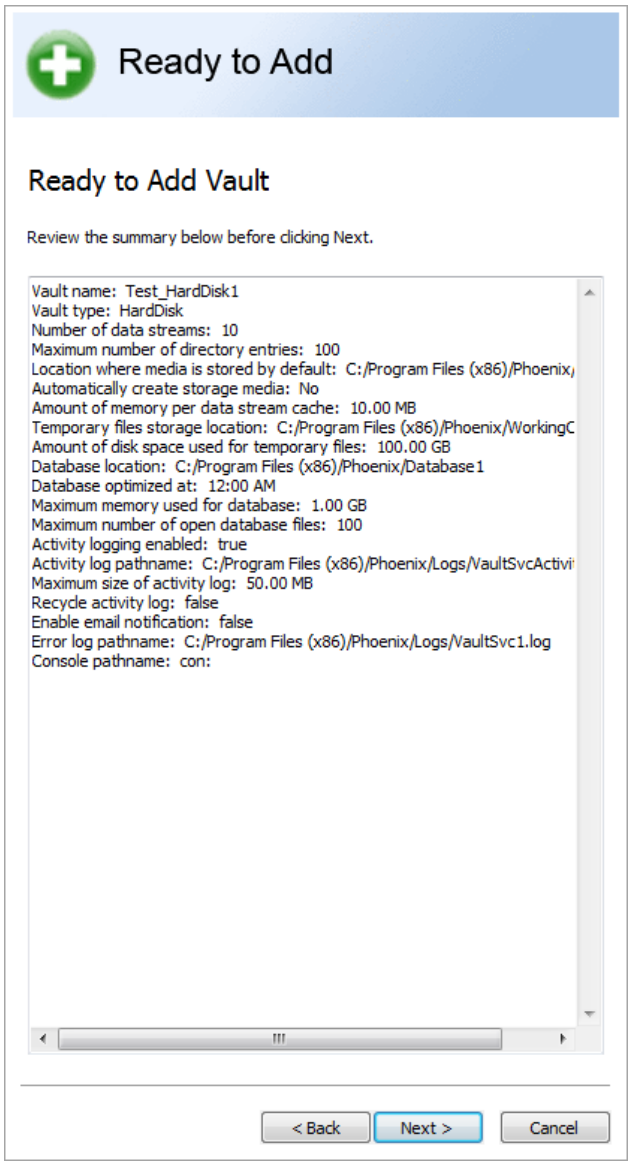



8. Click **Next** for the Ready to Add window. The Ready to Add window displays a summary of the Vault values. See the corresponding header for your storage device type:

Hard Disk Summary

- Review the displayed summary and ensure all the values are correct. If information is incorrect, click the **Back** button to navigate through previous wizard windows to edit.

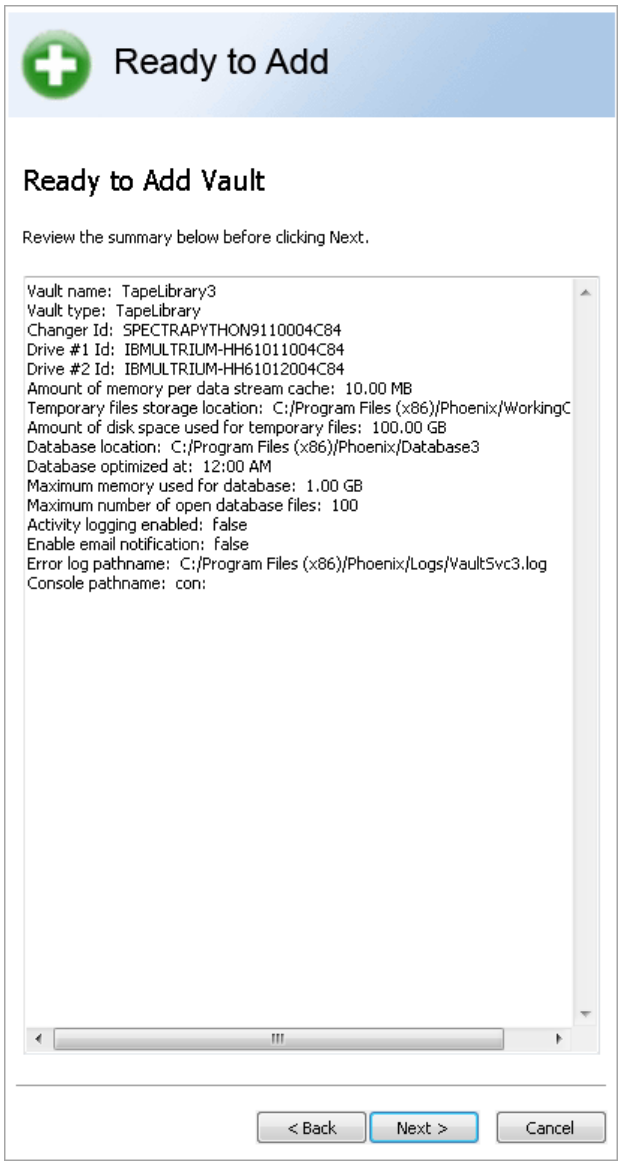
© 2015


Ready to Add
Ready to Add Vault
Review the summary below before clicking Next.
Vault name: Test_HardDisk1
Vault type: HardDisk
Number of data streams: 10
Maximum number of directory entries: 100
Location where media is stored by default: C:/Program Files (x86)/Phoenix/
Automatically create storage media: No
Amount of memory per data stream cache: 10.00 MB
Temporary files storage location: C:/Program Files (x86)/Phoenix/WorkingC
Amount of disk space used for temporary files: 100.00 GB
Database location: C:/Program Files (x86)/Phoenix/Database1
Database optimized at: 12:00 AM
Maximum memory used for database: 1.00 GB
Maximum number of open database files: 100
Activity logging enabled: true
Activity log pathname: C:/Program Files (x86)/Phoenix/Logs/VaultSvcActivi
Maximum size of activity log: 50.00 MB
Recycle activity log: false
Enable email notification: false
Error log pathname: C:/Program Files (x86)/Phoenix/Logs/VaultSvc1.log
Console pathname: con:
< Back
Next >
Cancel

Tape Library Summary

- Review the displayed summary and ensure all the values are correct. If information is incorrect, click the **Back** button to navigate through previous wizard windows to edit.

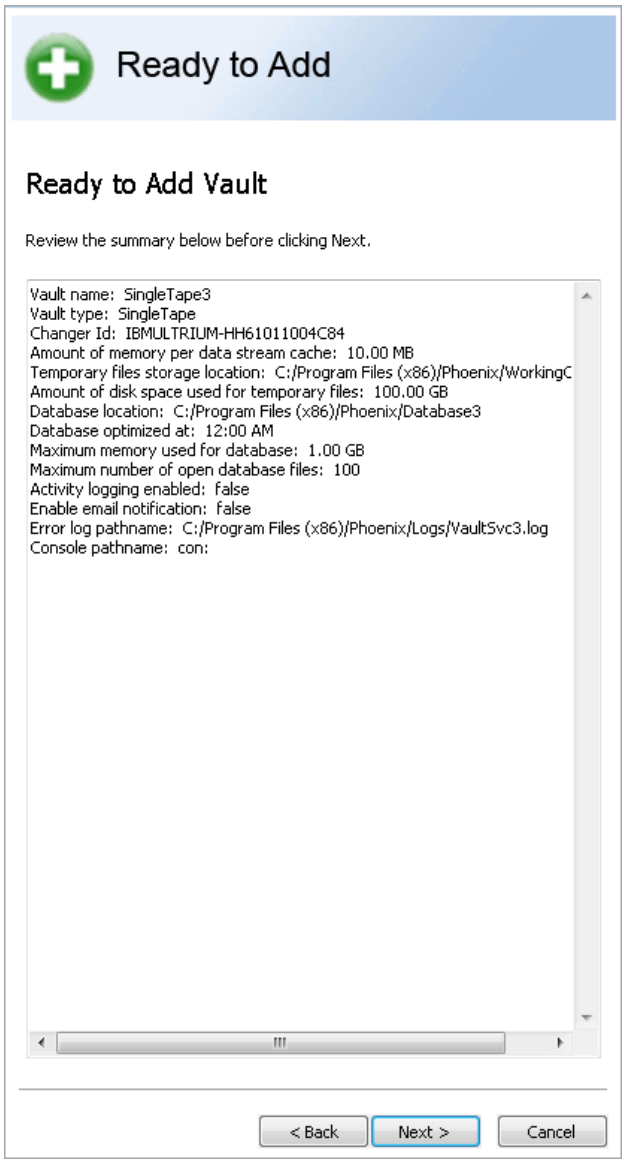
© 2015


Ready to Add
Ready to Add Vault
Review the summary below before clicking Next.
Vault name: TapeLibrary3
Vault type: TapeLibrary
Changer Id: SPECTRAPYTHON9110004C84
Drive #1 Id: IBMULTRIUM-HH61011004C84
Drive #2 Id: IBMULTRIUM-HH61012004C84
Amount of memory per data stream cache: 10.00 MB
Temporary files storage location: C:/Program Files (x86)/Phoenix/WorkingC
Amount of disk space used for temporary files: 100.00 GB
Database location: C:/Program Files (x86)/Phoenix/Database3
Database optimized at: 12:00 AM
Maximum memory used for database: 1.00 GB
Maximum number of open database files: 100
Activity logging enabled: false
Enable email notification: false
Error log pathname: C:/Program Files (x86)/Phoenix/Logs/VaultSvc3.log
Console pathname: con:
< Back
Next >
Cancel

Standalone Tape Drive Vault Summary

- Review the displayed summary and ensure all the values are correct. If information is incorrect, click the **Back** button to navigate through previous wizard windows to edit.

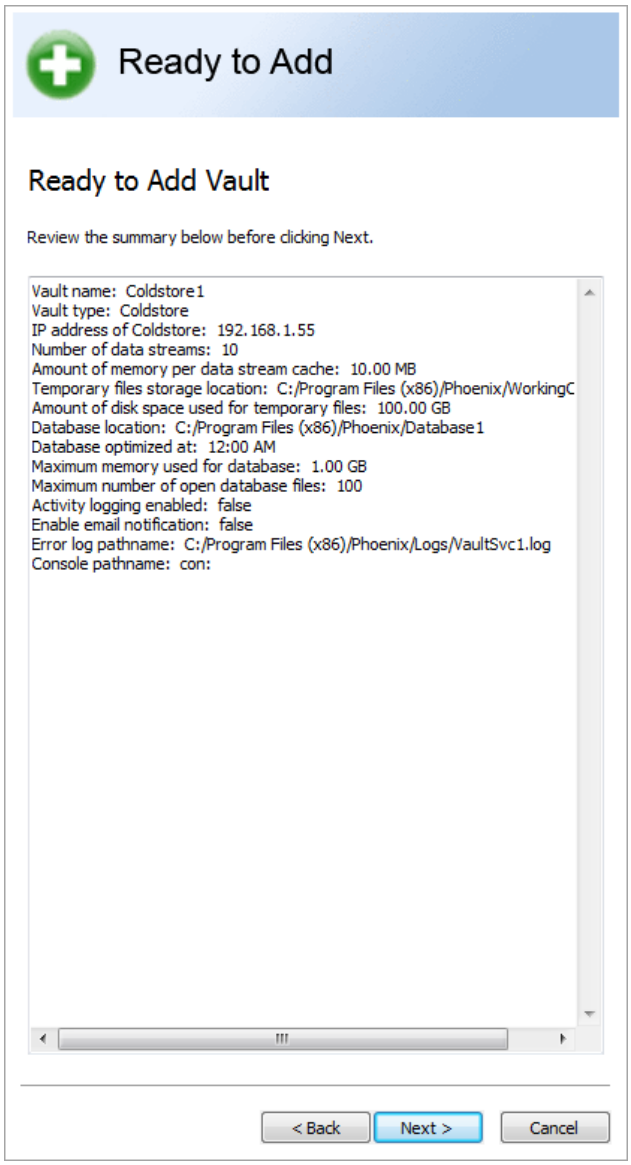
© 2015


Ready to Add
Ready to Add Vault
Review the summary below before clicking Next.
Vault name: SingleTape3
Vault type: SingleTape
Changer Id: IBMULTRIUM-HH61011004C84
Amount of memory per data stream cache: 10.00 MB
Temporary files storage location: C:/Program Files (x86)/Phoenix/WorkingC
Amount of disk space used for temporary files: 100.00 GB
Database location: C:/Program Files (x86)/Phoenix/Database3
Database optimized at: 12:00 AM
Maximum memory used for database: 1.00 GB
Maximum number of open database files: 100
Activity logging enabled: false
Enable email notification: false
Error log pathname: C:/Program Files (x86)/Phoenix/Logs/VaultSvc3.log
Console pathname: con:
< Back
Next >
Cancel

Veracity Coldstore Summary

- Review the displayed summary and ensure all the values are correct. If information is incorrect, click the **Back** button to navigate through previous wizard windows to edit.

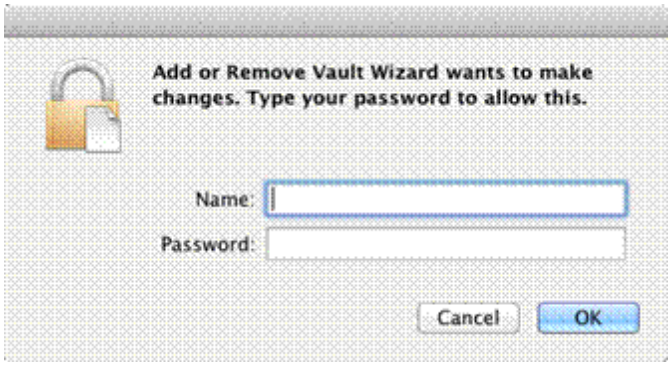
© 2015


Ready to Add
Ready to Add Vault
Review the summary below before clicking Next.
Vault name: Coldstore1
Vault type: Coldstore
IP address of Coldstore: 192.168.1.55
Number of data streams: 10
Amount of memory per data stream cache: 10.00 MB
Temporary files storage location: C:/Program Files (x86)/Phoenix/WorkingC
Amount of disk space used for temporary files: 100.00 GB
Database location: C:/Program Files (x86)/Phoenix/Database1
Database optimized at: 12:00 AM
Maximum memory used for database: 1.00 GB
Maximum number of open database files: 100
Activity logging enabled: false
Enable email notification: false
Error log pathname: C:/Program Files (x86)/Phoenix/Logs/VaultSvc1.log
Console pathname: con:
< Back
Next >
Cancel

9. When ready to add the new Vault, click **Next**.

    - Mac users will be prompted for an Administrator Name and Password. The Name field may already be populated with the name of the user running the Vault Wizard.

© 2015




- After entering a Name and Password, click **OK**. The Vault will start immediately.

  A restart is not required on a Mac.

10. In the Completed window, click **Finish** to exit the Add or Remove Vault Wizard. Restart the computer for the new Vault activation. To add another Vault or remove a Vault, launch the Add or Remove Vault Wizard again.

    If you do not restart your computer, the new Vault does not start and is not available for use.

11. The next step is to prepare your media using Vault Admin. See Prepare Media and Vault Admin.

## Disable SCSI Devices

If you are using Windows Vista or newer, or Windows Server 2008 or newer, you do not need to disable the use of SCSI devices.

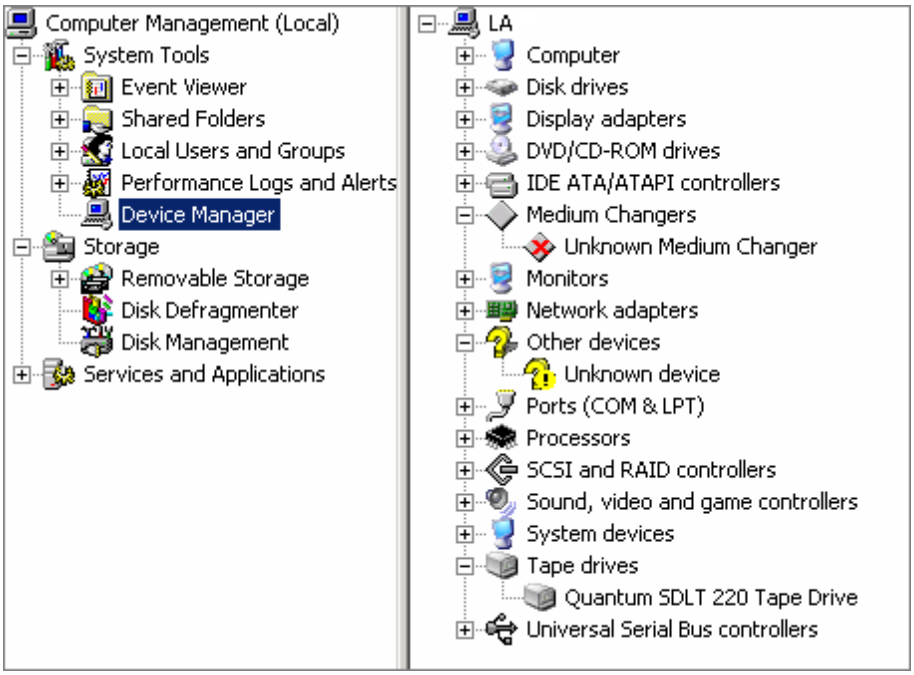
Disable the use of SCSI devices in a Windows environment to ensure that Windows does not interfere with Phoenix RSM's management of SCSI tape drives and libraries (Medium Changers). This is done through the Windows Device Manager.

- This procedure only disables Windows use of the device and does not affect Phoenix RSM's use of the device.
- Devices that are active (not disabled) in Windows are not visible or used by Phoenix RSM.

To access the Device Manager:

1. Click **Start** on the Windows desktop.
2. Right-click **My Computer** and select **Manage** from the shortcut menu. The **Computer Management** window appears.
3. In the left pane of Computer Management, click **Device Manager**:

© 2015

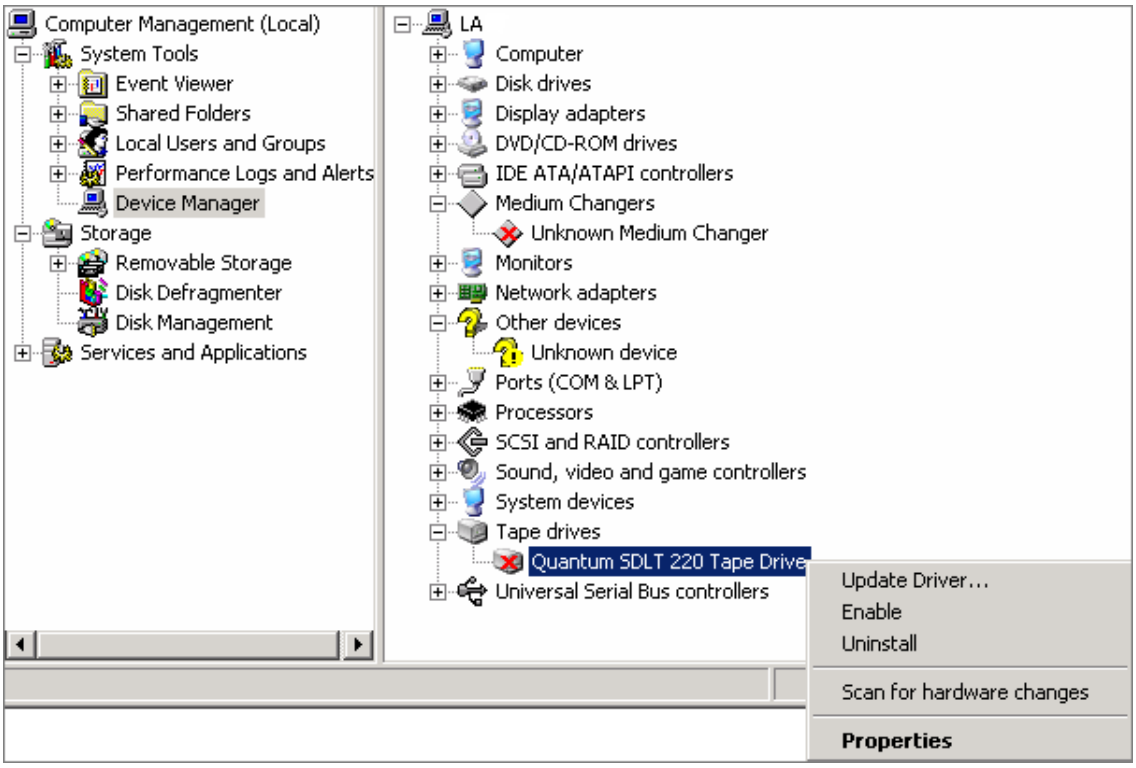



5. In the right pane, find the tape drive or tape library installed on the computer.

6. Right-click the tape drive, and then select **Properties**.

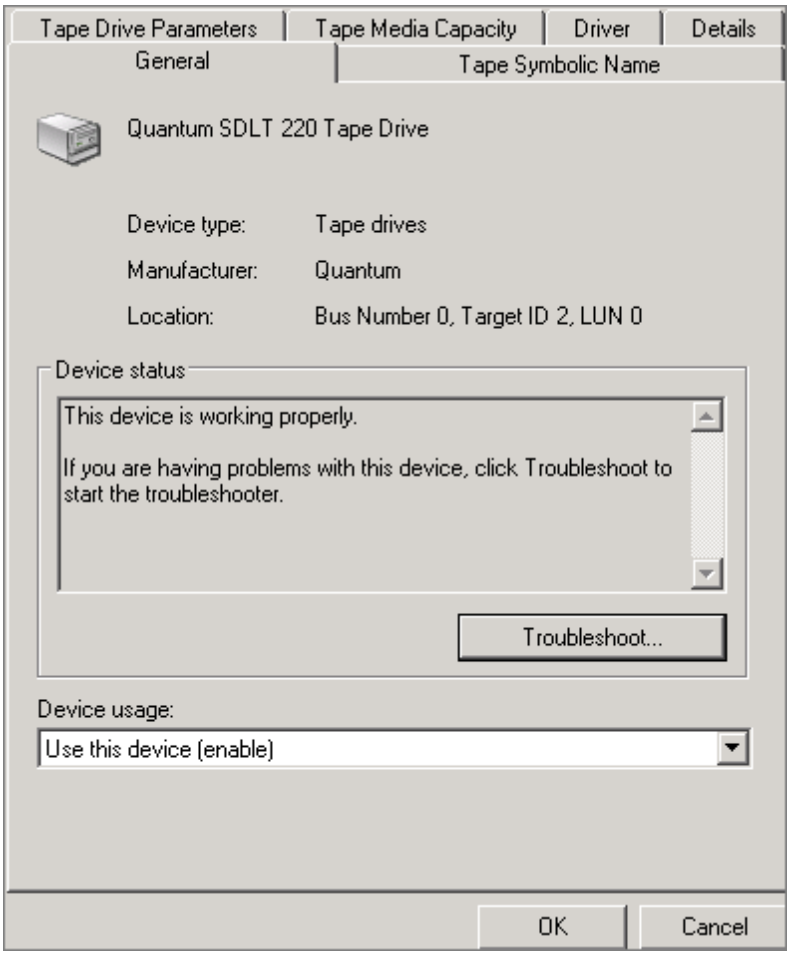
If running a tape library, be sure to disable the tape library (Medium Changers) and the actual tape drives in the library. Repeat the disabling process for each tape drive within the library.

© 2015




7. The **Tape Drive Properties** window appears:

© 2015




8. Under **Device Usage**, click the down arrow, and select **Do not use this device (disable)**.
9. Click **OK**. The **Tape Drive Properties** window closes, and the icon for the device in the right pane of **Computer Management** should now have ✗ superimposed on it to show the tape drive is disabled.

## Vault Admin

Use Vault Admin and the Vault Service to administrate added Vaults, manage video and storage, and to prepare media and manage media on your network. The Vaults can use different types of media to store all your video and data assets. The Vault Admin application can be installed anywhere and it can be used anywhere on the network.

© 2015

A Vault must be configured and running, and media must be prepared in order to do any other task.

To access the Vault Admin, from your suite of product applications open the Vault Admin application (VaultAdmin.exe).

## Vault Admin window

Vault Admin is divided into two main panes, and it has toolbar buttons across the top of the window. Most Phoenix RSM applications require you to interface through tab options, but with Vault Admin you use the menu items or toolbar. The left pane displays a list of the tracked Vaults and views, like a common file manager application. The right pane displays details for the object select from the left pane. The toolbar consists of the following buttons:

- Open Vault Stats for monitoring detailed Vault activity.

- Open Mini Vault Stats for monitoring basic Vault activity.

- Open the Vault Security dialog box. To secure a Vault means to lock it so no further media can be added to it.

- Open the Shut Down Vault dialog box for assigning a Vault offline. Take Vaults offline before performing any type of maintenance to the hardware where a Vault resides.

- Open Change Vault Properties. Define Vaults, devices, databases, licensing, diagnostics, notifications, logs, and security settings for Vaults.

- Open Vault Checkup. Run a Vault checkup to check the general health of a Vault.

- Open the Load Media dialog box. Bring previously prepared media back online.

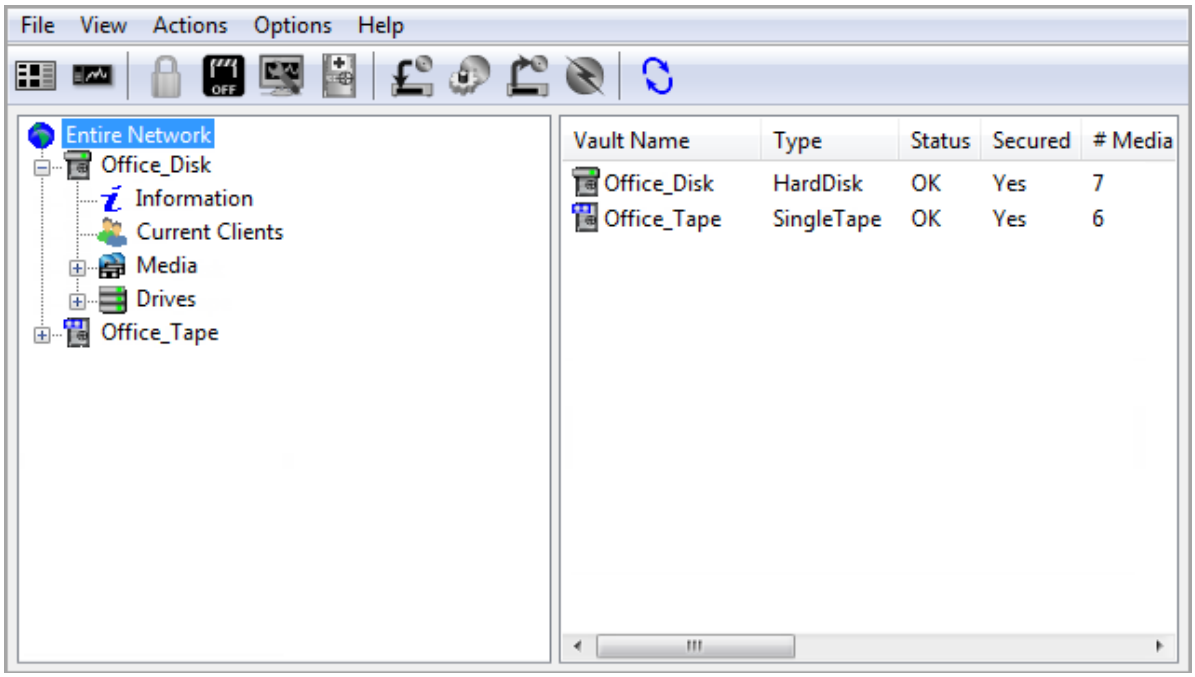
- Open the Prepare Media dialog box. Prepare new or previously used media.

- Open the Unload Media dialog box. Media can be removed from the Information Repository or labeled as offline, and be tracked by the Information Repository.

- Open the Erase Media dialog box. Remove all data from a unit of media without reformatting the media.

- Refresh the view of the currently displayed data; update the information in the Vault Admin.

© 2015




When performing Vault and media operations, the software may appear as if it is not responding. When the given task is completed, it responds normally.

Users that have unlimited rights and access to Vault resources are: UNIX "root". Windows "local group administrators", and Windows "backup operators".

## Vault Admin Menu Items

| Menu Items | Description |
|---|---|
| **File > Extended Metadata** | **Import from** - The Import from window opens. Navigate to the MetadataExtensions.cfg file that you wish to import. Click **Open**.<br><br>**Export to** - The Export to window opens. Navigate to the location where you want to export the MetadataExtensions.cfg file. Click **Save**. |
| **File > Exit** | Close the application. |
| **View > Enable toolbar** | Check mark by this menu item indicates that the toolbar is displayed. |

© 2015

| Menu Items | Description |
|---|---|
| **View > Enable Advanced** | Select to access advanced options for a Vault item. This advanced mode displays a couple of details:<br><br>**Volume** - This details volume information on media if the media has more than one volume associated with it. For example, a data tape might store data on both sides of the tape, presenting two volumes of media storage. If advanced mode is selected a Volume icon displays with Vault sub-items in the Vault Admin left pane.<br><br>**Shut down notifications** - In advanced mode, shut down methods present notifications of each event, which are time stamped and indicate the name of the Vault. (Not using advanced mode only displays one generic notification regardless of multiple events.) |
| **View > Enable Tool Tips** | Check mark by this menu item indicates that tool tips for the window display. The tips are brief descriptions of window controls that are displayed if the mouse pointer is moved over a control. De-select to turn tool tips off. |
| **View > Refresh** | Refresh the view of system information. |
| **Actions > Vault Stats** | Open Vault Stats for monitoring detailed Vault activity. |
| **Actions > Mini Vault Stats** | Open Mini Vault Stats for monitoring basic Vault activity. |
| **Actions > Secure/ Unsecure Vault** | Open the Vault Security dialog box. To secure a Vault means to lock it so no further media can be added to it. |
| **Actions > Shut Down Vault** | Open the Shut Down Vault dialog box for assigning a Vault offline. Take Vaults offline before performing any type of maintenance to the hardware where a Vault resides. |
| **Actions > Change Vault's Properties** | Open Change Vault Properties. Define Vaults, devices, databases, licensing, diagnostics, notifications, logs, and security settings for Vaults. |
| **Actions > Vault Checkup** | Open Vault Checkup. Run a Vault checkup to check the general health of a Vault. |
| **Actions > Load Media** | Open the Load Media dialog box. Bring previously prepared media back online. |
| **Actions > Prepare Media** | Open the Prepare Media dialog box. Prepare new or previously used media. |

© 2015

| Menu Items | Description |
|---|---|
| **Actions > Unload Media** | Open the Unload Media dialog box. Media can be removed from the Information Repository or labeled as offline, and be tracked by the Information Repository. |
| **Actions > Erase Media** | Open the Erase Media dialog box. Remove all data from a unit of media without reformatting the media. |
| **Options > Address Format** | Address format refers to the format that client addresses are displayed in the Vault Admin. Change the Address Format to see Current Client addresses displayed in a different format.<br>• Select one of the following address format view options:<br>**Dot Notation** - The client's computer network address is displayed.<br>**Full Domain Name** - The client computer is displayed along with the domain and subnet names.<br>**Host Name Only** - The client's host name and port number are displayed.<br> Use the **Refresh** button to redisplay the active clients. Right-click in the active window to activate the button. |
| **Options > Communications Timeout** | If unable to connect with a computer on the network or communications are interrupted during a job, Phoenix RSM waits a predefined period of time before completely dropping the connection. This period of time is called the communications timeout.<br>Set a higher or lower timeout wait value to better suit network conditions should communications between components fail or hang during a job.<br>• Select a timeout value for the Information Repository, 0 being shortest, 3 the default, 9 being longest, and 10 never. All values are relative.<br> The communications timeout value can impact the performance of other components. |
| **Help > Current Page** | Open online help to the Vault Admin webpage. |
| **Help > Vault Admin Overview** | Open online help with focus on Vault Admin. |

© 2015

| Menu Items | Description |
|---|---|
| **Help > Contents** | Open the local version of online help. |
| **Help > Online Help** | Open the web-based version of online help. |
| **Help > Online Support** | Open the support webpage. |
| **Help > About Vault Admin** | Open the About Vault Admin window. |

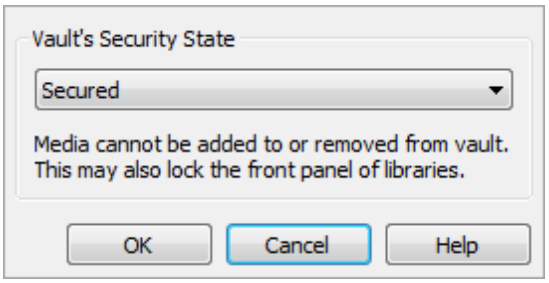
## Vault Secure or Unsecure

Use the Vault Security dialog box to protect your Vaults in your Information Repository. Vaults should normally be run in a secured mode, where a Vault's media cannot be manipulated. Media cannot be imported or exported, copied, reformatted, or even relabeled. In Vaults equipped with storage devices that can be locked via software, the front panel and all access panels are locked when the Vault is operating in secure mode.

Before any media operation can be performed, such as preparing media, a Vault must be unsecured.

To secure or unsecure a Vault:

1. From the Vault Admin left pane, select a Vault name.
2. From the toolbar, click the **Secure/Unsecure Vault** button.




3. From the Vault Security dialog box, use the drop-down list to select either **Secured** or **Unsecured**.

   **Secured** - Media may be added to and removed from a Vault based on access rights to the media.

   **Unsecured** - Media cannot be added or removed from Vault. This may also lock the front panel of libraries.

4. Click **OK** to complete the process.

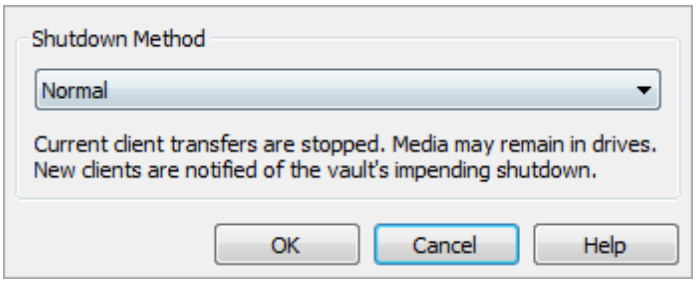
© 2015

## Vault Shutdown or Restart

Use the Shut Down Vault dialog box to shut down or restart a selected Vault. Shutting down a Vault must be performed before you can modify the Vault's host computer.

To shut down or restart a Vault:

1. From the Vault Admin left pane, select a Vault name.
2. From the toolbar, click the **Shut Down Vault** button.




3. From the Shut Down Vault dialog box, use the **Shutdown Method** drop-down list to select between three ways to shut down a Vault and one way to restart a Vault.

   **Normal** - Normal shutdown is the standard way to shut down a Vault. A Normal shutdown stops current client activity after the running transaction completes all database transactions and performs any cleanup activity required, but it does not remove media from the drive. A Vault restarted after a normal shutdown should not report errors.

   **Extended** - Extended shutdown is the best way to shut down a Vault if it is going to be taken offline for an extended period of time. Phoenix RSM waits until running client processes are finished before closing connections to clients, and then completes all database transactions, removes media from drives, and performs any required cleanup activity. An Extended shutdown is more time consuming than a Normal shutdown.

   **Restart** - Restart executes a Normal shutdown and then restarts the selected Vault. Client activity stops after the running transaction completes all database transactions and performs any cleanup activity required, but does not remove media from the drive.

   **Emergency** - Use only for emergencies. The emergency shutdown behaves as if removing power from the host computer. A Vault restarted after an emergency shutdown may report connection timeouts, incomplete database translations, and other items.

4. Click **OK** to complete the process.

## Vault Properties

After Vault installation, use Vault Properties to change Vault settings. Properties to modify includes general settings, security, logs, notifications, diagnostics, memory allocation for devices, database optimization parameters, and licensing.

To access Vault Properties:

© 2015

1. Open the Vault Admin application. In the left pane of the Vault Admin main window, select a Vault to modify.

2. From the Vault Admin toolbar, click the **Change Vault's Properties** button to launch the <Vault Name> Properties window, or right-click on the selected Vault name and select **Properties**. The Properties window features several tabs; each responsible for some aspect of Vault functionality. It opens to the **General** tab.

Vault Properties opens to the **General** tab by default. From the following tabs, select one to bring its properties into focus for modification:

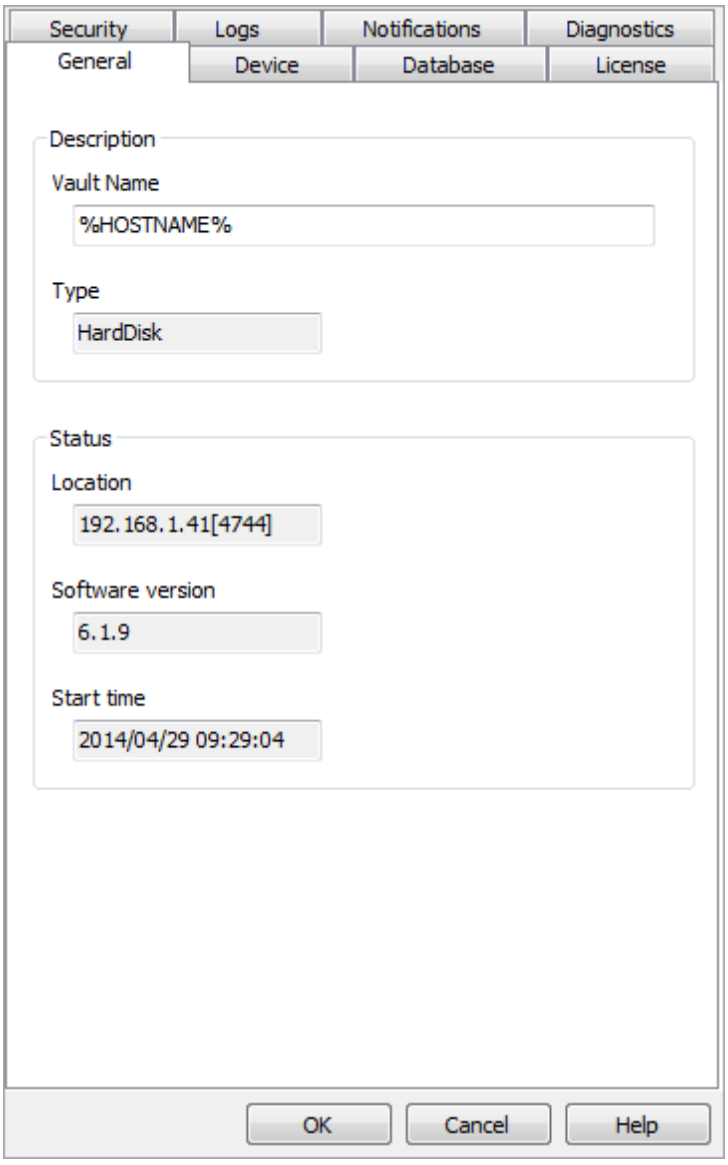
- **General** - Rename the Vault and view the Vault type and status information, including location, software version, and start time.
- **Device** - View SCSI information for Vaults as well as maximum files kept in a directory and maximum number of data streams. Also, change the amount of virtual memory used for each data stream cache for Vaults.
- **Database** - View the database path. Also, change the time when the database is optimized, set the number of maximum open files, and set the amount maximum virtual memory used.
- **License** - Access your Host Id and view installed licenses and license summary. Activate a product key, and change, delete or import a license file.
- **Security** - Define Vault access for users, groups, and domains.
- **Logs** - Activate activity logging, define an activity log path, set maximum log size, set what action to take when logs reach their maximum size, and define where error logs go.
- **Notifications** - Set where events and e-mail notifications are sent.
- **Diagnostics** - Define where output messages are sent, the type of messages sent, and the level of message detail.

### Vault Properties General Tab

Use the Vault Properties **General** tab to change the overall settings of a Vault. Here, you can modify the Vault name and view the Vault type, location, software version of Phoenix RSM, and Vault start time.

Access this from Vault Properties by clicking the **General** tab.

© 2015




1. Change the selected Vault's name, and type a new name in the **Vault Name** box.
2. Click **OK**, and the new Vault name is listed under **Entire Network** in the Vault Admin left pane.

## General Tab Elements

| Element | Description |
|---|---|
| **Vault Name** | The name of the Vault. You can change the name of the Vault at any time. The entered name appears in the Vault Admin left pane under **Entire Network**. |

© 2015

| Element | Description |
|---|---|
| | Rather than hard coding a Vault Name, use the variables **%HOSTNAME%** and **%TYPE%**. **%HOSTNAME%** is replaced by the computer name and **%TYPE%** is replaced by the type of Vault. |
| **Type** | Read only box, displaying the type of device. |
| **Location** | Read only box, displaying the IP address of the device. |
| **Software version** | Read only box, displaying the software version of Phoenix RSM. |
| **Start time** | Read only box, displaying the time when the Vault was first started. |

#### Vault Properties Device Tab

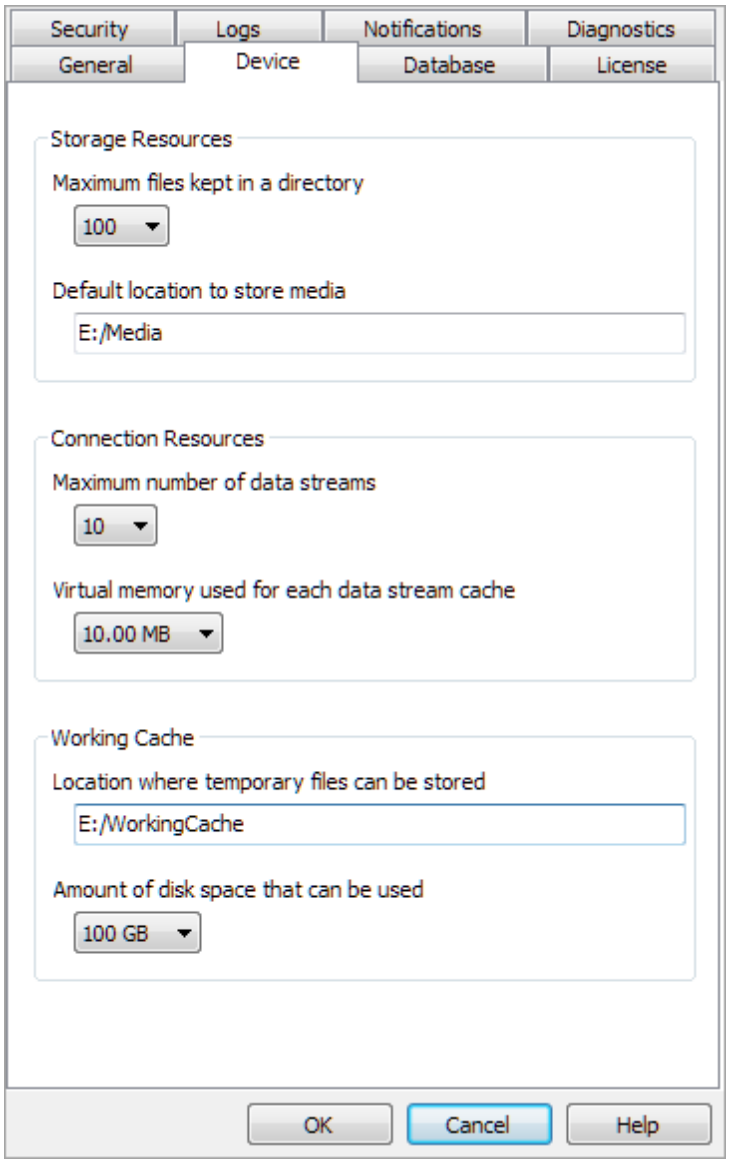
Use the **Device** tab to change the selected Vault's storage connection resource settings. The values displayed on this tab change depending on if you've selected a hard disk Vault or a data tape Vault.

Access this from Vault Properties by clicking the **Device** tab.

1. Select preferred Vault values.
2. Click **OK** to save new settings.

## Hard Disk Vault

© 2015

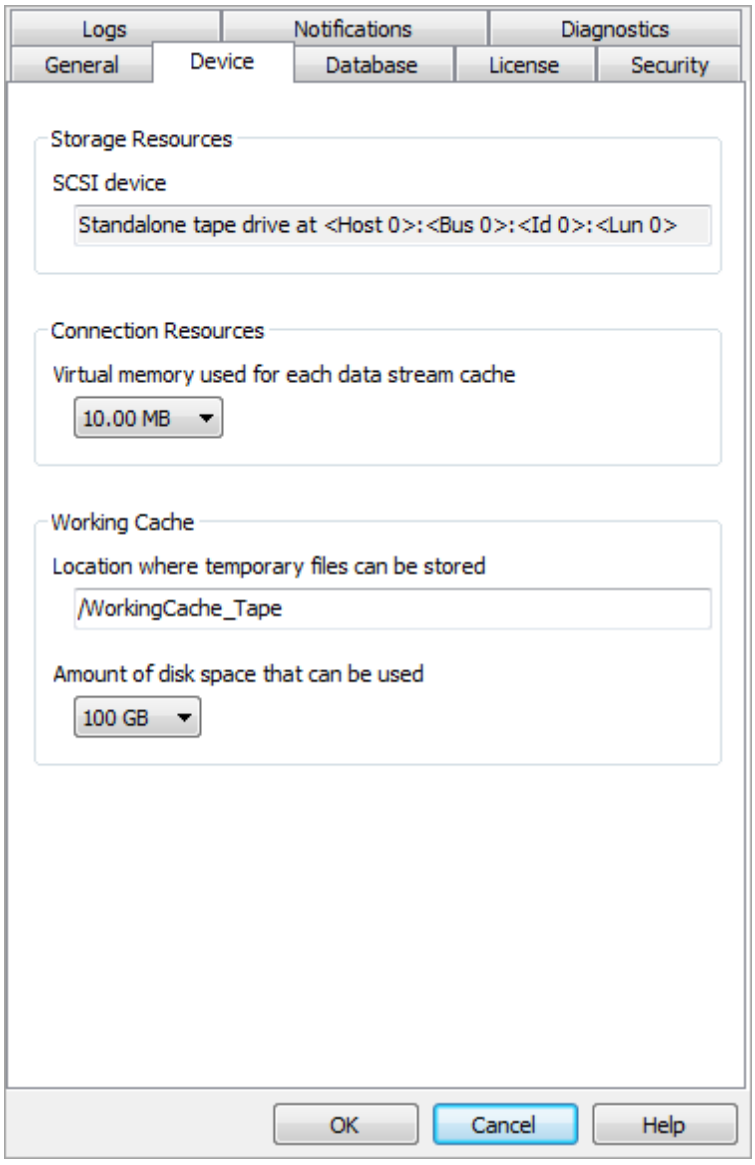



## Data Tape Vault

On the **Device** tab for data tape Vaults, change only the amount of virtual memory used for each data stream cache.

**SCSI device** is a read only box. It indicates the hardware in use and where it is located on the network.

© 2015




## Device Tab Elements

Use this table to help change the values for the appropriate Vault type. Note that not all elements are available for each type of Vault.

© 2015

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>Maximum files kept in a directory</td><td>Data is stored in files in the Vault. More files allow more storage per unit of media, but also slow down Information Repository performance. Select a value to meet but not exceed your needs. The following details the number of files that correlates with each value.
<table>
<tr><th>Value</th><th>Number of Files</th></tr>
<tr><td>50</td><td>125 billion</td></tr>
<tr><td>100</td><td>250 billion</td></tr>
<tr><td>150</td><td>375 billion</td></tr>
<tr><td>200</td><td>500 billion</td></tr>
<tr><td>300</td><td>750 billion</td></tr>
<tr><td>400</td><td>1 trillion</td></tr>
<tr><td>500</td><td>125 trillion</td></tr>
</table></td></tr>
<tr><td>Default location to store media</td><td>Define a default location where media is stored and managed. Whenever there is an option to use a default location, Phoenix RSM uses this path.</td></tr>
<tr><td>Maximum number of data streams</td><td>The number of connections that can be made to a Vault simultaneously. Having several connections enables several clients to communicate with the Vault at once; more streams demand greater requirements for processing power. Range:1 - 50.</td></tr>
<tr><td>Virtual memory used for each data stream cache</td><td>Define how much virtual memory is set aside for incoming and outgoing data during file storage and retrieval. A larger cache may improve performance, at the expense of using more virtual memory. The total amount of space used equals the number of data streams multiplied by the selected cache size.<br><br>For example, with 10 data streams and 10 MB of cache, the Vault sets aside 100 MB of total virtual memory for caching data. A selection of 10 MB is usually sufficient. Range: 5, 10, 15, 20 MB.</td></tr>
</table>

© 2015

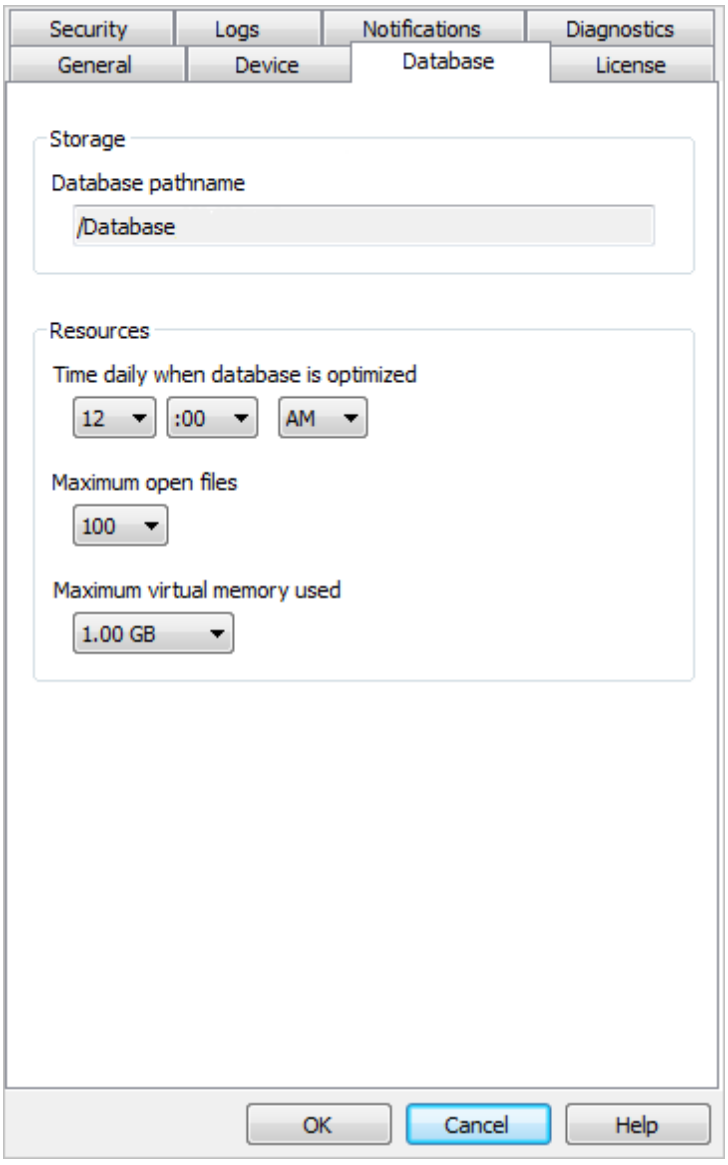
| Element | Description |
|---|---|
| **Location where temporary files can be stored** | Define where the working cache is located. The default location is '<install-dir>/WorkingCache'.<br><br>When processing files, Phoenix RSM may create temporary files, which enable fast, efficient work and are important for clipping video files. Temporary files are kept in the working cache.<br><br> Any changes will override the values entered when you first added the Vault using the Add or Remove Vault Wizard. |
| **Amount of disk space that can be used** | Define the amount of disk space permitted to use for the working cache. Range: 10 - 900 GB |

### Vault Properties Database Tab

Use the **Database** tab to allocate resources for a Vault database. Select when a Vault is optimized, the maximum number of files to open at a single time, and the amount of virtual memory the Vault uses.

Access this from Vault Properties by clicking the **Database** tab.

© 2015




1. Select preferred Vault values.
2. Click **OK** to save new settings.

## Database Tab Elements

| Element | Description |
|---|---|
| **Database pathname** | Defined when installing a Vault. It indicates the location where the database is stored on the host computer's hard disk. |

© 2015

| Element | Description |
|---|---|
| **Time daily when database is optimized** | Set how often the database is optimized to ensure that the Information Repository continues to function at its full potential. It is recommended to optimize the database for every Vault daily. |
| **Maximum open files** | Limit how many files can be open simultaneously. Having more files open allows for faster searches, but requires more Information Repository resources. Range: 10 - 500 |
| **Maximum virtual memory used** | Limit how much virtual memory the database uses. For best Information Repository performance, select a value that does not exceed 75% of the physical memory on the computer. Range: 256 MB - 2 GB |

### Vault Properties License Tab

Get a licensed product from SoleraTec. You can purchase a licensed product online or download a trial version from SoleraTec's website. By default, this product comes with a seven day evaluation license. At the end of the evaluation period, you can request an extended evaluation product key or purchase a product license through the same sales channels. For more information see Product Licensing.

If you run the software longer than seven days with an evaluation license, your Vaults will shut down or your cameras will no longer be tied to the software. Until a license is purchased and added, the Vaults run in increments of only two hours.

From Vault Properties, use the **License** tab to manage Vault licenses.

- The **Summary** group displays your license totals for the selected Vault.
- The **Host Id** group displays the Vault Host Id. The Host Id information is used to activate your product key.
- The **Installed Licenses** group displays all the individual licenses assigned to a Vault. The license statistics shown are Serial #, Type, Capacity, Expiration, Product Type, and Platform Type. Click the **Add** button to open the Add License window where you can add a new license by activating a product key, or import a license file. Select an installed license from the group and then click the **Delete** button to remove the license from the Vault.

Once the **Add** or **Delete** button is clicked, the changes are immediate.

You can add the same license as many times as you like, but the Vault Admin just overwrites the license file so only one instance is displayed in the **Installed Licenses** group.

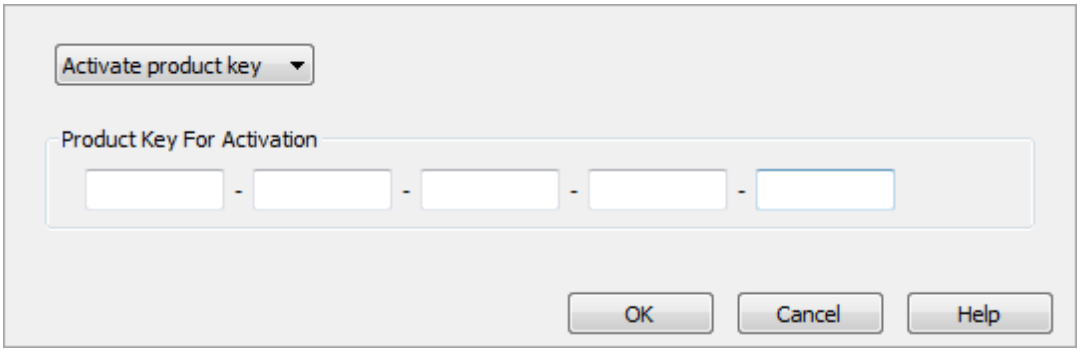
## Add license and activate product key - Connected to Internet

© 2015

Once you have received your product key, and you are connected to the Internet, follow the steps below to activate your license.

1. Open the Vault Admin application. In the left pane of the Vault Admin main window, select a Vault to modify.
2. From the Vault Admin toolbar, click the **Change Vault Properties** button to launch the <Vault Name> Properties window, or right-click on the selected Vault name and select **Properties**. The Properties window features several tabs; each responsible for some aspect of Vault functionality. It opens to the **General** tab.
3. Select the **License** tab.
4. Click the **Add** button. When the Add window appears, select **Activate product key** drop-down menu. Begin typing the product key into the appropriate boxes, or copy and paste the product key into the first box. It will propagate the appropriate boxes automatically.

When using Mac, the copy and paste action is not carried out properly. To ensure the product key is entered correctly, manually type in the product key to the appropriate box.

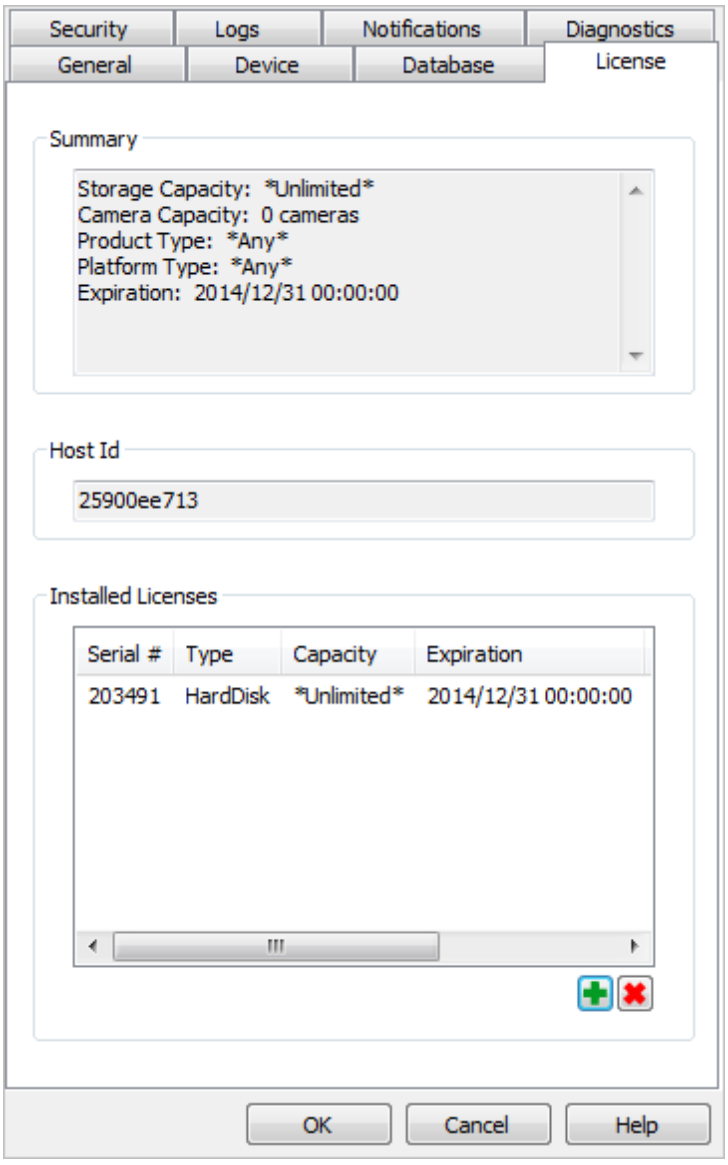



## Add license and activate product key - Not connected to Internet

If you have received a product key, and are not connected to the internet, follow these steps:

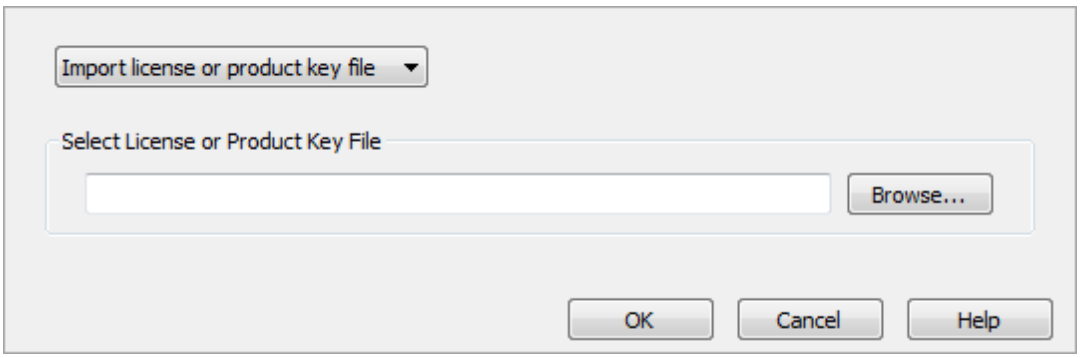
1. Find a computer with internet access.
2. Go to SoleraTec's website and locate the product key activation page.
3. Type your Host Id, e-mail, and product key. The Host Id is located in Phoenix RSM, from the <Vault Name> Properties > **License** tab, as shown in the image below. The product will run for up to two hours regardless of license status, so you still have access to the Vault Admin. You may need to reboot your computer to initiate the product.

© 2015




4. A license file will be sent to you via e-mail.

5. After receiving the license file, from <Vault Name> Properties > **License** tab, click the **Add** button.




© 2015

6. From the Add License window, select **Import license or product key file** from the drop-down menu.
7. Type, or click the **Browse** button to navigate to the received license file, **.lic**, or a product key file, **.pk**.
8. Click **Ok** to complete manual activation.

If you are having problems activating your license, visit the SoleraTec website for manual activation.

## Licensing options on website

**Download** - Select a product and download it with an evaluation license, which is good for seven days.

**Purchase** - If connected to the internet, buy a product. This provides you with a product key. Once the product key is entered into the product key information, it pulls a license file to your machine and activates it automatically.

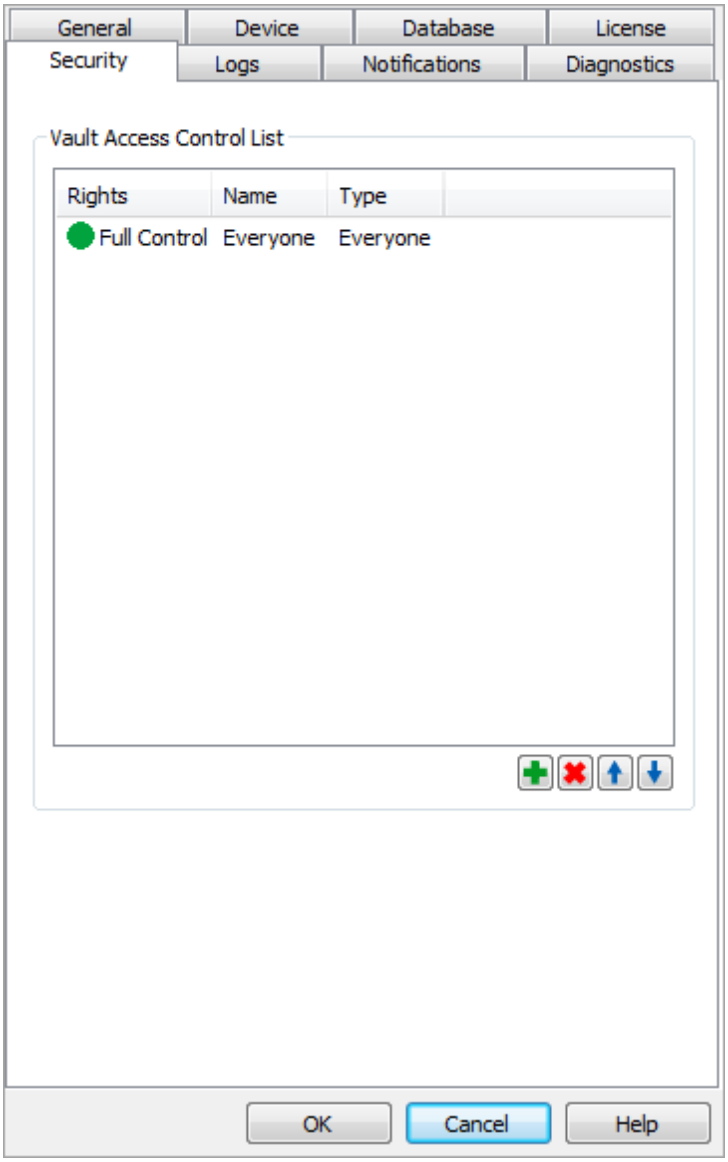
**Activate** - Use if you already have a product key and your computer is not connected to the internet. Find a computer with internet access and submit your Host Id. A license file will be sent to you to import it into the product.

© 2015

### Vault Properties Security Tab

Use the **Security** tab to add, change, and delete user, group, and domain rights for the selected Vault. Vault rights override media rights, see Prepare Media.

Access this from Vault Properties by clicking the **Security** tab.




1. Add, change, or delete security rights.
2. Click **OK** to save new settings.

## Security Tab Elements

© 2015

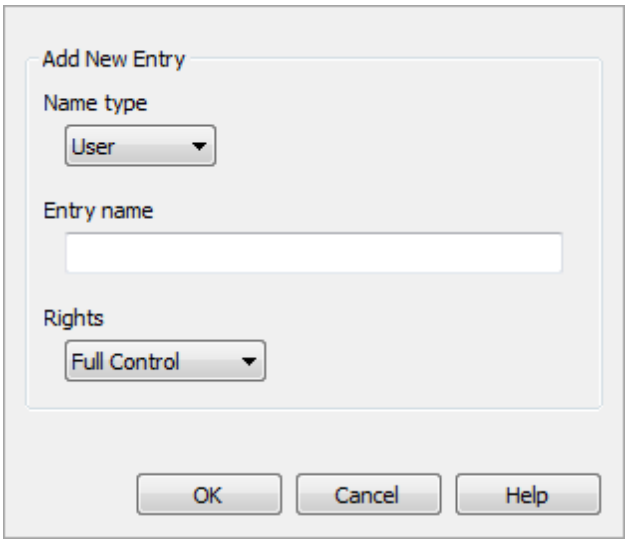
| Element | Description |
|---|---|
| **Vault Access Control List** | Click on a right in the list to select it, or double-click on a right for the Change Entry window.<br><br>View the columns:<br><br>**Rights** - The level of rights given to user, group, domain, or everyone.<br><br>● - Indicates full rights.<br><br>◓ - Indicates rights to store and retrieve data.<br><br>○ - Indicates rights to retrieve (but not store) data.<br><br>✕ - Indicates no rights.<br><br>**Name** - Name of the user, group, domain, or everyone.<br><br>**Type** - The Type of rights. |
| (**Add** button) | Open the Add Entry dialog box. Use to add a new user, group, domain, or "everyone". See **Add Entry** section below. |
| (**Delete** button) | Remove the selected right from the Vault Access Control list. |
| (**Up** button) | Move the selected right up one line in the Vault Access Control list. |
| (**Down** button) | Move the selected right down one line in the Vault Access Control list. |

## Add Entry

Use the Add Entry dialog box to add a new user, group, domain, or everyone.

1. Click the **Add Entry** button.

© 2015




2. From the **Name Type** drop-down list, select a type of right. Rights are granted to the entity selected. The type of right can be **User**, **Group**, **Domain**, or **Everyone**.

3. In the **Entry Name** box, type a name for the new entry. This name appears in the **Name** column. The name entered must be valid for the computer where the Vault is running.

4. From the Rights drop-down list, select the actual rights granted to the given user, group, domain, or everyone. The following are the selections:

   **Full Control** - Allows the user, group, domain, or everyone to have full control over a selected Vault.

   **Store/Retrieve** - Allows the user, group, domain, or everyone to store and retrieve data from the Vault.

   **Retrieve** - Allows user, group, domain, or everyone to retrieve (but not store) data from the Vault.

   **None** - Blocks the user, group, domain, or everyone from doing anything with the Vault.

5. Click **OK**.

6. Use the up and down arrows to move the new entry up or down in the list to change the priority the new entry is given in relation to other users, groups, and domains.

   Phoenix RSM reads rights from top to bottom, checking for access in the following order: User, Group, Domain, World. If a match is found at the User level, the other types (Group, Domain, World) are not checked; if a match is not found at the User level, the Group entries will be checked, starting with the topmost Group entry in the list. The same pattern holds true for the remaining types. Note that Vault rights and media rights are hierarchical, with media rights being subordinate to overall Vault permissions.

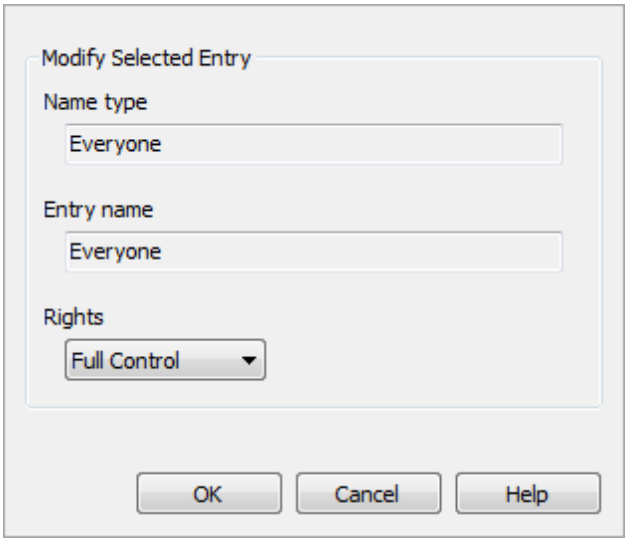
7. Repeat the steps above to add even more entries, or click **OK** to save them.

© 2015

## Change Entry

Use the Change Entry dialog box to modify rights for an entry.

1. Double-click the entry to change, and the Change Entry dialog box appears. The **Name Type** and **Entry Name** boxes are not editable.




2. From the **Rights** drop-down list, select the actual rights granted to the given user, group, domain, or everyone. The following are the selections:

   **Full Control** - Allows the user, group, domain, or everyone to have full control over a selected Vault.

   **Store/Retrieve** - Allows the user, group, domain, or everyone to store and retrieve data from the Vault.

   **Retrieve** - Allows user, group, domain, or everyone to retrieve (but not store) data from the Vault.

   **None** - Blocks the user, group, domain, or everyone from doing anything with the Vault.

3. Click **OK** to save changes.

4. From the main window, click **OK** to save changes.

## Delete Entry

1. To remove an entry from a list, select it.

2. Click the **Delete** button, and the entry deletes.

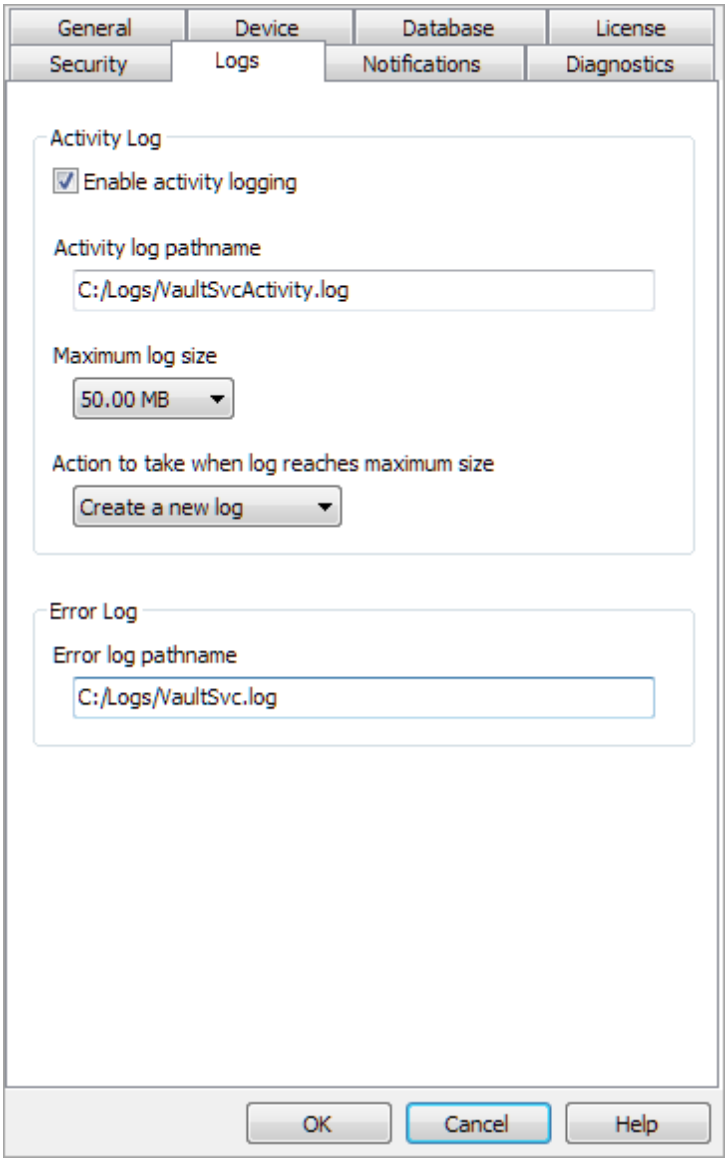
3. Click **OK** to save changes.

© 2015

### Vault Properties Logs Tab

Use the **Logs** tab to set parameters and log activity for the selected Vault.

Access this from Vault Properties by clicking the **Logs** tab.




1. Select preferred Vault values.
2. Click **OK** to save new settings.

## Logs Tab Elements

© 2015

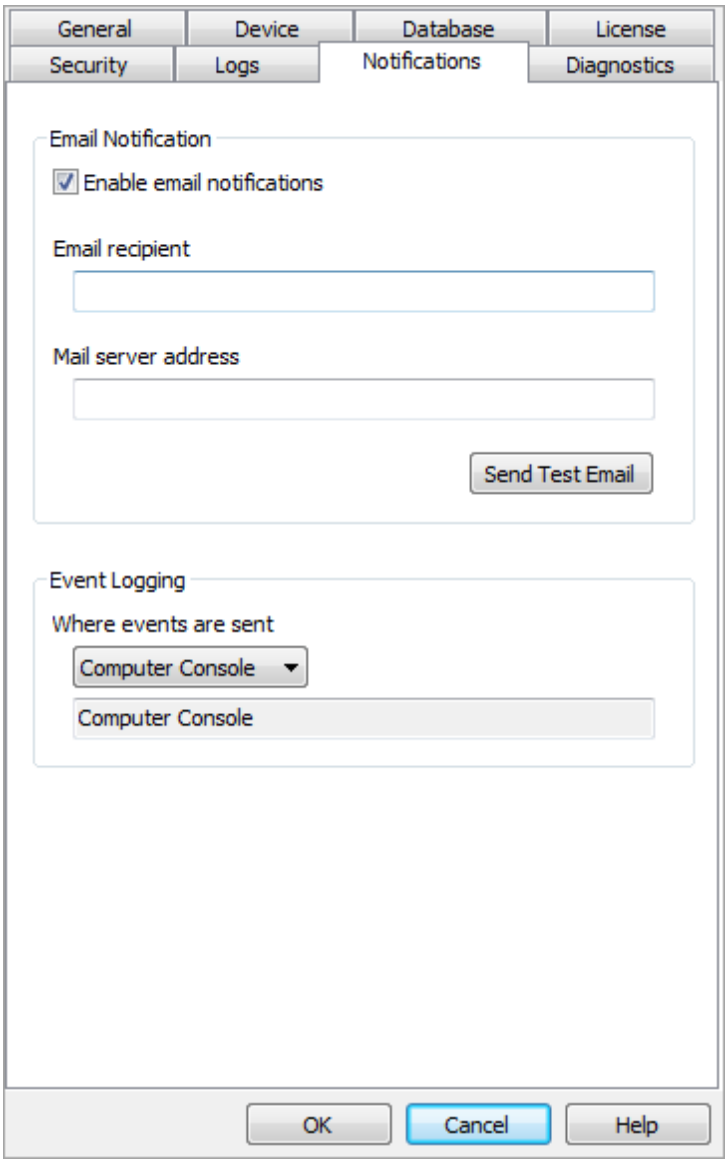
| Element | Description |
|---|---|
| **Enable activity logging** | Select to enable activity logging and the activity log boxes for this Vault Properties tab. If not selected, no activity logs are created.<br><br>Phoenix RSM provides a security audit trail through activity logs. Activity logs include the following events: Vault start, Vault stop, file read, file write, file create, file delete, media load, media unload, and media erase. For these events the name and IP address of the user who executed the event and the date and time the event was executed is recorded.<br><br>Activity logs can be imported into any application that supports a tab-delimited format, such as Microsoft Excel. |
| **Activity log pathname** | Define where the activity logs are written to. |
| **Maximum log size** | Define the maximum size the activity log can become. Limit the size of the activity log to find needed information quickly; in large logs this becomes more difficult. Range: 25 MB - 1 GB |
| **Action to take when log reaches maximum size** | Either select **Overwrite existing log** or **Create a new log**. Overwriting the activity log prevents activity log build-up. |
| **Error log pathname** | Define where error logs are stored. Where activity logs record all activity, error logs record only events that have gone wrong.<br><br>Error logs are created only when a Vault encounters a problem. Error logs include warnings, and Vault start and stop information. Phoenix RSM supports error logging for every Vault in the Information Repository, and error logging is always enabled. |

### Vault Properties Notifications Tab

Use the **Notifications** tab to set how Phoenix RSM event notifications are published by enabling and defining e-mail. Events include anything of interest for managing a Vault, including Vault start, Vault stop, media requests, etc.

Access this from Vault Properties by clicking the **Notifications** tab.

© 2015




1. Select preferred Vault values.
2. Click **OK** to save new settings.

## Notifications Tab Elements

| Element | Description |
|---|---|
| **Enable e-mail notification** | Enable optional e-mail notifications and boxes from this Vault Properties tab. |

© 2015

| Element | Description |
|---|---|
| | When enabled, receive an e-mail when an event occurs for managing a Vault. These events include Vault start, Vault stop, media requests, etc., and are the same as those recorded for notifications. |
| **E-mail recipient** | Type the e-mail address of the user receiving e-mail notifications about Phoenix RSM events. |
| **Mail server address** | The address of your mail server. Use either IP address or computer name.<br>• Click the **Send Test E-mail** button to test the path.<br> If an invalid IP address or computer name is typed, e-mail notifications do not work. |
| **Where events are sent** | Define where events are logged.<br>**Computer Console** causes events to be logged in a console that appears on the computer monitor. It remains open as long as the Vault is running. If the Vault is stopped, the console disappears. If the Vault is restarted, the console disappears and then reappears.<br>**Window** causes events to be logged in a window that appears on the computer monitor. This window remains open as long as the Vault is running. If the Vault is stopped, the window disappears. If the Vault is restarted, the window disappears and then reappears.<br>**File** causes events to be logged to a file. Type the path where you want events logged.<br>If a window or console is open when changing the mode of output to **File**, the console or window closes, but the Vault continues to run.<br>To configure the Vault Service to open a window for diagnostic messages see Windows Diagnostics. |

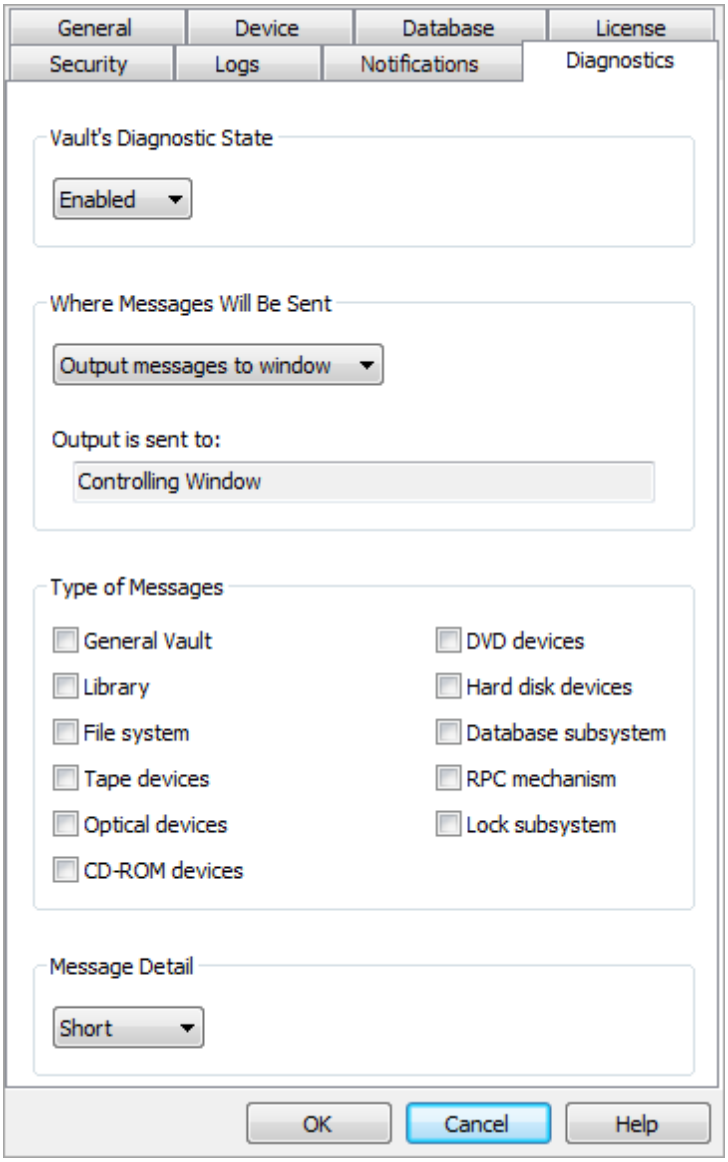
© 2015

### Vault Properties Diagnostics Tab

Use the **Diagnostics** tab to run diagnostic logs for the selected Vault. When enabled, diagnostic logs are created for all Vault activity. Diagnostic logging is optional, and since it significantly impacts system performance, it is disabled by default. Diagnostic logs output to a window or console by default, and if you restart the Vault and return to this tab, diagnostic logs are set to the default of **Disabled**.

If you use diagnostic logging to assist in the resolution of problem conditions, be aware that it seriously impacts Information Repository performance. This is a complex feature and should be used with discretion.

Access this from Vault Properties by clicking the **Diagnostics** tab.




1. From the **Vault's Diagnostic State** drop-down list, select **Enable**.

2. Select preferred options.

3. Click **OK** to save new settings.

## Diagnostics Tab Elements

| Element | Description |
|---|---|
| **Where Messages will be sent** | Select from the following options:<br><br>**Output messages to window** - Sends the output information to a controlling window that is opened by the process.<br><br> With this option, a window appears to display Vault activity. If you close this window, you stop the Vault, and Phoenix RSM does not operate without running Vaults.<br><br> Working in Windows: To configure the Vault Service to open a window for diagnostic messages see Windows Diagnostics.<br><br>**Output messages to file** - Type the path (including the file name) where you want message files written. This option creates a file that contains all the output data. |
| **Output is sent to** | Define where **Output is sent to**. The file path (including the file name) typed here defines where message files are written to. This option creates a file that contains all of the output data. |
| **Type of Messages** | Select the types of devices to capture diagnostic information from. Select the checkbox in front of each option; you can make multiple selections. The following are message results for each device:<br><br>**General Vault** - Information about client connections and data moving in and out of the Vault.<br><br>**Library** - SCSI activity regarding moving media within a robotic data tape storage device.<br><br>**File System** - Host computer's working environment.<br><br>**Tape Devices** - Information about the storage device itself.<br><br>**Optical Devices** - Information about the storage device itself. |

© 2015

| Element | Description |
|---|---|
| | **CD-ROM Devices** - Information about the storage device itself.<br><br>**DVD Devices** - Information about the storage device itself.<br><br>**Hard Disk Devices** - Information about the storage device itself.<br><br>**Database Subsystem** - For use only by Phoenix RSM engineers.<br><br>**RPC Mechanism** - For use only by Phoenix RSM engineers.<br><br>**Lock Subsystem** - For use only by Phoenix RSM engineers. |
| **Message Detail** | Select the level of detail of diagnostic logs.<br><br>**Short** - Provides only high-level overview information about the issues being tracked. For example, the General Vault feature only contains client connection names.<br><br>**Standard** - Provides some detail about the issue being tracked. For example, the General Vault feature provides additional information about the client connection times, and connection types. The Standard option is recommended.<br><br>**Extended** - Provides a full set of details. It is usually reserved to assist in resolving complex issues in low-level Information Repository functions. |

## Vault Checkup

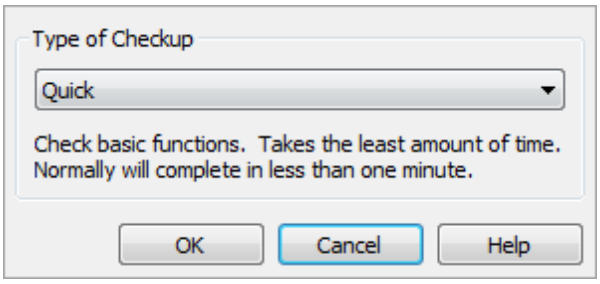
Use the Vault Checkup dialog box to view the health of a Vault. This tool is great to use if you suspect something may be wrong with a Vault in your Information Repository.

To run a Vault checkup, Vault Admin requires at least one piece of media with available space and that it does not belong to a storage pool.

To run a Vault checkup:

1. From the Vault Admin left pane, select a Vault name.
2. From the toolbar, click the **Vault Checkup** button.

© 2015




3. From the Vault Checkup dialog box, select from the drop-down list a level of check to run. Each level examines the Vault function, speed, and load bearing capacity to some degree.

   **Quick** - Check basic functions and takes the least amount of time. Normally completes in less than one minute.

   **Normal** - Check commonly used functions. Best tradeoff of time and complexity. Normally completes in five minutes.

   **Extensive** - Exercise the Vault for functionality and speed. Normally completes in ten minutes.

4. Click **OK** to complete the process. Upon completion, a Vault Checkup output window appears containing the results of the checkup.

## Prepare Media

Use the Prepare Media window to add and load media to your Information Repository. All the parameters can be set to prepare a unit of media to use with a Vault. Some of these parameters cannot be changed unless you reformat the media (see Prepare Existing Media). Depending on the type of media, the Prepare Media window appears with slight differences.

Before you can prepare media, Vaults should already be added to your Information Repository. Remember that the Vault to add media to must be unsecured before you can prepare any media. To add Vaults, see Add Vaults.

### Prepare New or Unknown Media

Follow these steps to prepare **new** or **unknown** media:

Some vaults, such as tape libraries or standalone tape, will show media labeled **Unknown_xx** (with **xx** representing a number). This is referred to as **unknown media**. These are removable media which are not known to the vault you are connected. Media in this state can be unprepared (new) media, media from another vault that is not indexed, or media with an unknown format.

Preparing an Unknown media will erase all existing data.

1. From the Vault Admin left pane, click the expand indicator (plus sign) in front of the Vault to add media to.

© 2015

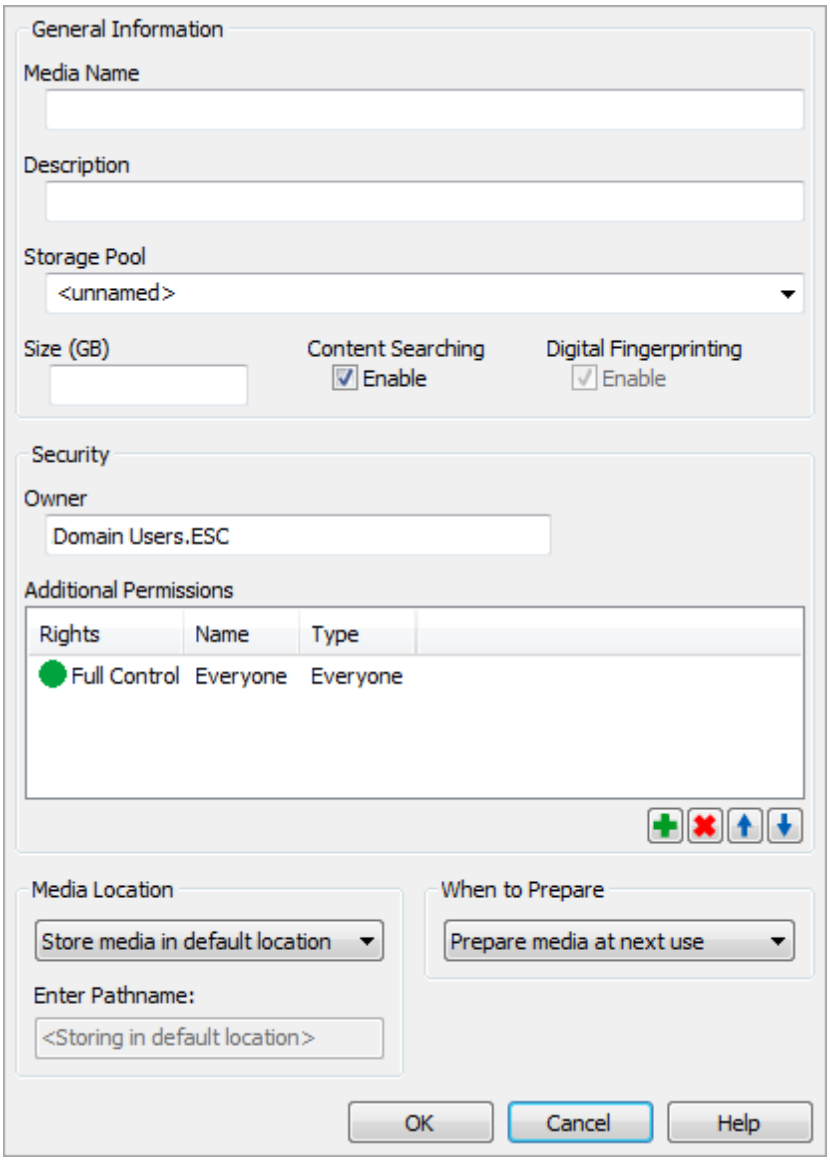
2. To prepare **new media, c**lick on **Media** then click on the **Prepare Media** button in the toolbar. Or right-click on **Media** and choose **Prepare Media** from the shortcut menu. To prepare **unknown** media, click on the expand indicator in front of **Media** to display all media in a tree. Click on the **unknown** media in the tree then click on the **Prepare Media** button in the toolbar. Or right-click on the selected **unknown** media and choose **Prepare Media** from the shortcut menu.

   - You can prepare multiple **Unknown Media** at one time by holding the **Shift** key or **Control** key and clicking on the desired media.

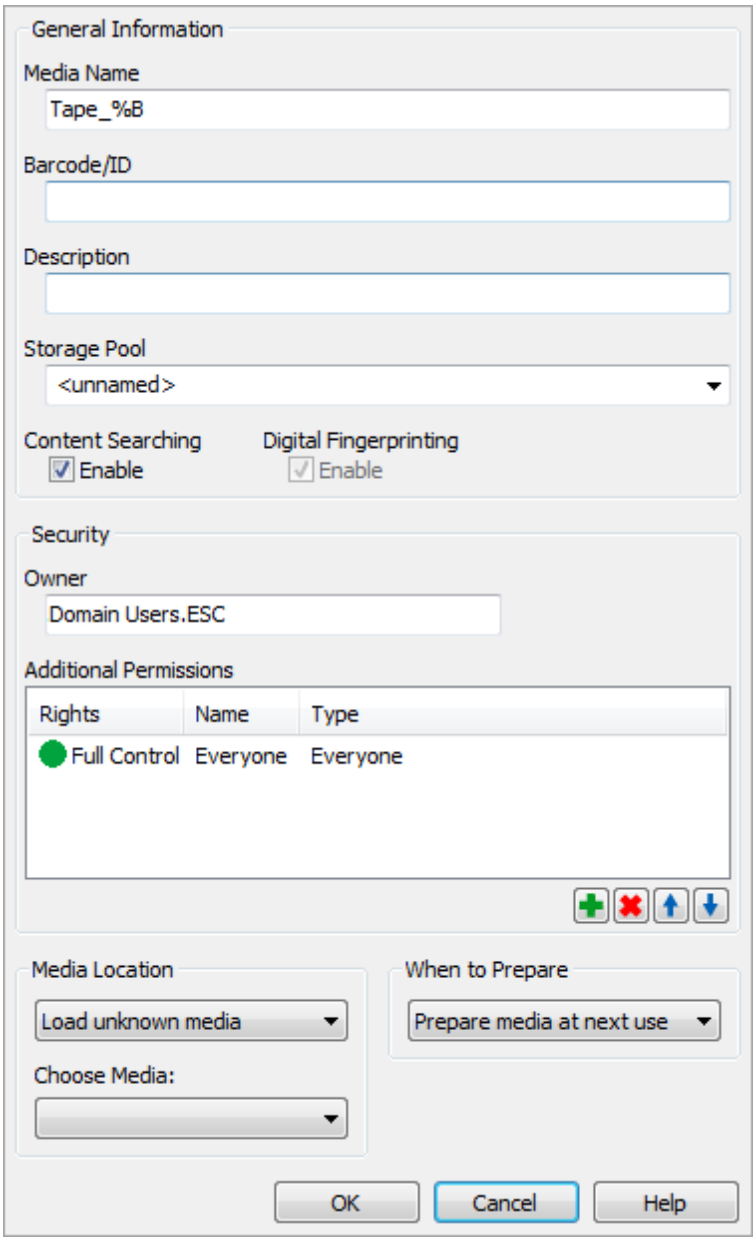
   Currently, you can only prepare multiple **tape** media. If you try to prepare multiple media that is not **tape**, you will receive an error message.

3. The options in the Prepare Media window are based on the media type of the Vault selected. In the screenshots below, the first displays disk media options for media being prepared for hard disk. The second image displays tape media options for media being prepared for data tape.

© 2015


General Information
Media Name
Description
Storage Pool
<unnamed>
Size (GB)
Content Searching
Enable
Digital Fingerprinting
Enable
Security
Owner
Domain Users.ESC
Additional Permissions
Rights
Name
Type
Full Control
Everyone
Everyone
Media Location
Store media in default location
Enter Pathname:
<Storing in default location>
When to Prepare
Prepare media at next use
OK
Cancel
Help

© 2015




4. Enter values into the Prepare Media window fields. Only **Media Name** and **Size** (only **hard disk**) are required. The information entered for **Media Name** and **Storage Pool** appear in the Data Service Policy **Source** tab, and in the **Destination** tabs of Camera Policies, and Data Service Policies.

5. In the **Additional Permissions** box, optionally assign rights to a user, group, domain, or everyone. For more information see Vault Properties Security tab, Add Entry.

6. From the **Media Location** drop-down list, assign a place to store new media.

7. From the **When to Prepare** drop-down list, assign a preparation time for the media.

8. Click **OK** to prepare the media with your selections.

© 2015

## Prepare Media Elements

| Element | Description |
|---|---|
| **Media Name** | This is the Information Repository reference name for the media. The name displays on all media referencing interfaces and reports. It is recommended to use a descriptive name to easily distinguish the unit of media.<br><br>The default name when preparing **existing tape media** is **Tape_%B**. This default name can be changed.<br><br> When **%B** is included in the media name of a **tape**, the **%B** will be replaced by the tape's barcode.<br><br> When preparing **multiple tapes**, **%B** must be used in the media name to avoid duplicate naming issues. |
| **Barcode/ID**<br><br>(Available for tape media that support barcodes) | This number corresponds to the barcode or a unique ID for the media. If used, Phoenix RSM tracks the media by its barcode.<br><br> Barcode systems provide a significant performance increase whenever media is being loaded, unloaded, or indexed by the Information Repository. |
| **Description** | Used on all media-referencing interfaces and reports. For easy identification, it is recommended to incorporate the naming convention used for the Media Name in the description. |
| **Storage Pool** | Storage pools are used to group disparate units of media. They are advantageous for performing multiple jobs at once and for preventing incomplete processing.<br><br>An example storage pool uses several units of media (which can be in different Vaults) together for use by a single policy. If you needed to have a "Monday night backup" write to several units of media, you would create a "Monday night backup" storage pool and assign to it every piece of media for that purpose. To assign media to a storage pool, select a storage pool from the **Storage Pool** drop-down list or type the name of the storage pool. |
| **Size (GB)**<br><br>(Available for hard disk media) | Define the amount of storage space to make available for the Information Repository on the given unit of media. |

© 2015

| Element | Description |
|---|---|
| | You can limit how much physical space on a single hard disk the Information Repository uses. For example, if the media has a physical capacity of 100 GB, you can limit the amount available to the Information Repository to 50 GB by typing 50. Values greater than the amount of space available are not accepted. |
| **Content Searching** | Search the content of files in the Information Repository.<br><br>Enable this feature to run content specific searches. Enabling this feature increases the size of your Vault's database. If not selected, you cannot search for content in your Information Repository. |
| **Digital Fingerprinting** | This option supports chain of custody management. When enabled, a digital fingerprint is assigned to all data captured or ingested into the Information Repository. This option is always selected and cannot be changed for hard disk and tape Vaults. |
| **Owner** | A read-only box, naming the owner of the media. The media owner value is from the Vault's host computer and the login used. |
| **Additional Permissions** | Permissions, or rights, are the limitations set for users and determine how users are permitted to manipulate files. Each piece of media can have up to sixteen different permission levels. The permissions information entered creates an access control list for the media.<br><br>For new media, all users on the network are granted rights to use media by default. To restrict access to media for specific users or groups, the default rights must be deleted, and then the new, limited rights need to be added.<br><br>To add new permissions, change existing permissions, or delete existing permissions, and for more information see Vault Properties Security tab. |
| **Media Location** | Options differ depending on if you are preparing a hard disk or tape media.<br><br>**Hard Disk**<br><br>• Leave the default location, **Store media at default location**. (This location is set when the Vault is first added, and can be changed using the Vault Properties **Device** tab for the Vault.)<br><br>Or, |

© 2015

| Element | Description |
|---|---|
| | 1. Select **Store media at pathname** to store media at a location other than the default.<br>2. In **Enter Pathname**, type a path including the drive letter of the location to store media related files and directories. For example, C:/Archive/SaturdayBackups.<br> When typing a path, the parent folder must already exist and no other media can be loaded at that same path. This path is relative to the computer where the Vault Service is running. The Vault Service must have rights to add files and folders at the specified location.<br>**Tape**<br>• Select **Load unknown media** and then from the **Choose Media** drop-down list, select the media.<br>Or,<br>• Select **Load from storage slot**, and then from the drop-down list, select a storage slot.<br>Or<br>• Select **Load from mail slot**, and then from the drop-down list, select a mail slot. |
| **When to Prepare** | Select a preparation time for the media.<br>**Prepare media at next use** - Media is prepared when a job is started that requires the selected media.<br>**Prepare media now** - Specified media is loaded into a drive and formatted immediately, regardless of when a job starts. |

## Prepare Existing Media

Preparing existing media is exactly like preparing media, as described in the above (Prepare Media) section, with only a few differences.

- You can use the Prepare Media option to reformat existing media. This will erase all current information stored on that media.
- Preparing existing media reformats media on tape and hard disk.

© 2015

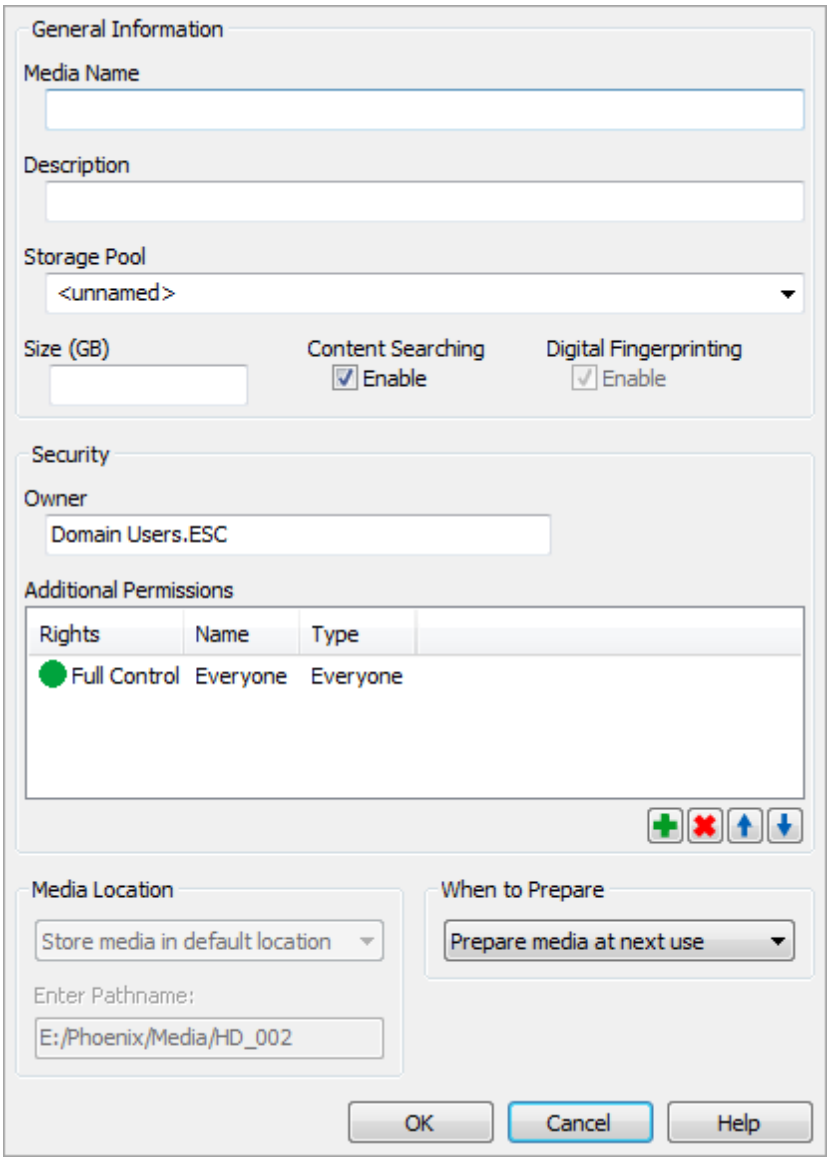
- Before reformatting media (or re-preparing media), be sure to first create and run a Data Service policy to migrate or move any data to a safe place if you want to preserve existing information on the media.
- The **Prepare Media** > **Media Location** option is not available when preparing existing media.

Follow these steps to prepare **existing** media:

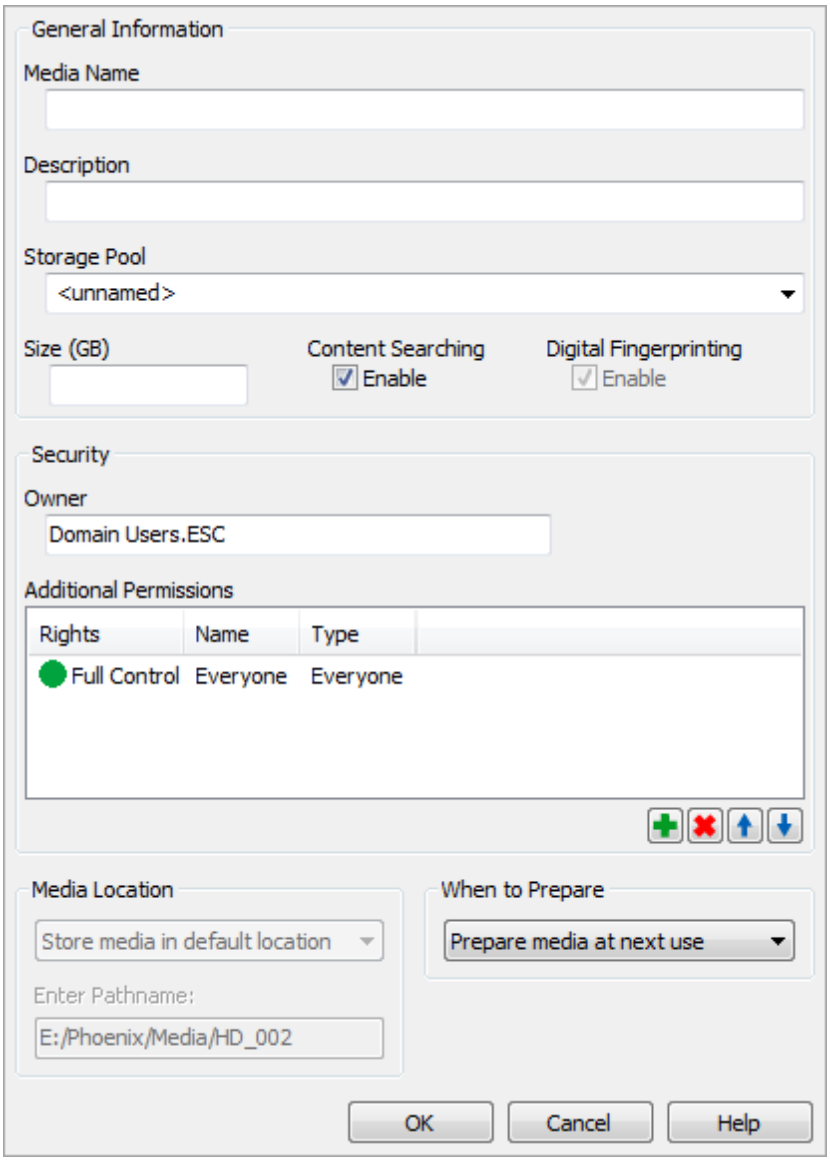
1. From the Vault Admin left pane, click the expand indicator (plus sign) in front of the Vault to add media to.
2. Click on the expand indicator for **Media** to have a tree of the **Media Names** displayed and also to have a list of the media names displayed in the right pane.
3. Select desired media (individual media or multiple **tape**) then click on the **Prepare Media** button in the toolbar. Or right-click on the selected media and choose **Prepare Media** from the shortcut menu.
   - You can prepare multiple **Media** at one time by holding the **Shift** key or **Control** key and clicking on the desired media.

   Currently, you can only prepare multiple **tape** media. If you try to prepare multiple media that is not **tape**, you will receive an error message.
4. The options in the Prepare Media window are based on the media type of the Vault selected. In the screenshots below, the first displays disk media options for media being prepared for hard disk. The second image displays tape media options for media being prepared for data tape.

© 2015


General Information
Media Name
Description
Storage Pool
<unnamed>
Size (GB)
Content Searching
Enable
Digital Fingerprinting
Enable
Security
Owner
Domain Users.ESC
Additional Permissions
Rights
Name
Type
Full Control
Everyone
Everyone
Media Location
Store media in default location
Enter Pathname:
E:/Phoenix/Media/HD_002
When to Prepare
Prepare media at next use
OK
Cancel
Help

© 2015




5. Enter values into the Prepare Existing Media window fields. Only **Media Name** and **Size** (only **hard disk**) are required. The information entered for **Media Name** and **Storage Pool** appear in the Data Service Policy **Source** tab, and in the **Destination** tabs of Camera Policies, and Data Service Policies.

If multiple **tapes** are selected, **%B** should be included in the name to avoid duplicate naming issues.

6. In the **Additional Permissions** box, optionally assign rights to a user, group, domain, or everyone. For more information see Vault Properties Security tab, Add Entry.

7. The **Media Location** section is not available when preparing existing media.

8. From the **When to Prepare** drop-down list, assign a preparation time for the media.

© 2015

9. Click **OK** to save your options.

### Media On The Fly

Increase automatic fail-over performance with the flexible Information Repository design to eliminate a single point of failure. If there is more than one Vault available, clients can divide use of the available Vaults. They can fail-over to other Vaults should a Vault fail. The same logic applies if there is more than a single tape-based Vault containing tapes with the same label.

For example, you can move media freely between Vaults of the same type. If a tape is taken out of one Vault and inserted into another, the Information Repository automatically locates the data. If a tape library is full, a second library can be brought online seamlessly. The result is a balanced Information Repository with two libraries that are accessible to the network.

## Load Media

Manage your media by loading media, reloading media, or re-indexing media. Use each in the following ways:

© 2015

**Load Media**

- To add previously created media to a Vault.
- To re-load media that has been ejected at some point in time and is not tracked.

If you attempt to load unprepared media to a Vault, the operation will fail.

**Reload Media**

- To add offline, but tracked media back to the Information Repository.

When reloading media, the Vault uses its database for the media unless it finds corruption (or re-indexing is forced). Use to reload media to the Vault. See Reload Media.

**Re-index Media**

- Rescan data on the media.

If media becomes unreliable then re-index it. To re-index media, first unload the media and then reload the media; otherwise the operation fails and an error message appears.

## Loading Media Types

The following subsections instruct you on how to load a hard disk media, a data tape media, and a shadow hard disk media.

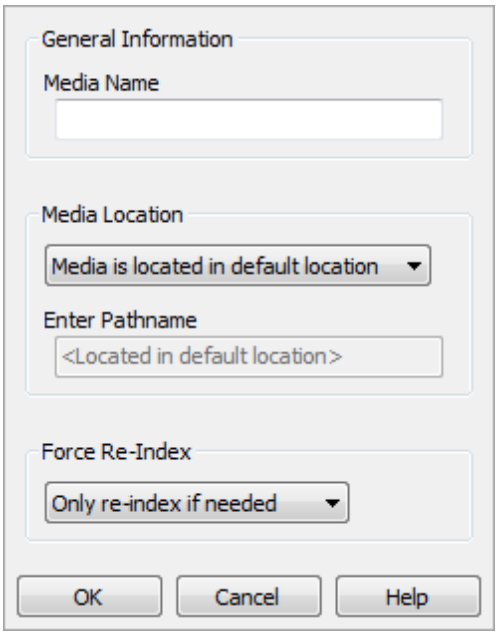
### Load Hard Disk Media

Load media to existing Vaults only. If you have not yet added any Vaults, do so now by using the Add or Remove Vault Wizard.

1. From the Vault Admin left pane, click the expand indicator (plus sign) in front of the Vault to load media to.
2. Click on the expand indicator for **Media** to have a tree of the media names displayed and also to have a list of the media names displayed in the right pane.
3. Select desired media (individual or multiple) then click on the **Load Media** button in the toolbar. Or right-click on the selected media and choose **Load Media** from the shortcut menu. The **Load Media** window opens.

You can load multiple hard disk media by holding the **Shift** key or **Control** key and clicking on the desired hard disk media in the right pane.

© 2015




4. In the **Media Name** text box, type the name for the media being loaded.
5. From the **Media Location** drop-down list, select **Media is located in default location** or **Media is located at pathname**. Know that Phoenix RSM always looks for the media at the default location.
6. If you select **Media is located at pathname**, type the directory path for the media being loaded in the **Enter Pathname** text box.
7. From the **Force Re-Index** drop-down list, use the default setting **Only re-index if needed**. Phoenix RSM indexes the media if necessary, but you can force re-indexing to ensure that your media is re-indexed by selecting **Force a re-Index of media**.
8. Click **OK** to complete the process, and new media appears in the media list.

## Load Tape Media

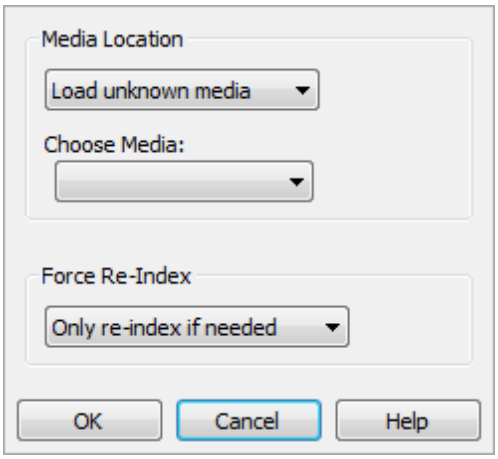
Load media to existing Vaults only. If you have not added Vaults yet, do so now using the Add or Remove Vault Wizard.

1. Ensure that there is a new media in the storage device. How to do this varies depending on the hardware being used. Refer to the hardware documentation for assistance.
2. From the Vault Admin left pane, click the expand indicator (plus sign) in front of the Vault to load media to.
3. Click on the expand indicator for **Media** to have a tree of the media names displayed and also to have a list of the media names displayed in the right pane.
4. Select desired media (individual or multiple) then click on the **Load Media** button in the toolbar. Or right-click on the selected media and choose **Load Media** from the shortcut menu. The **Load Media** window opens.

© 2015

You can load multiple tape media by holding the **Shift** key or **Control** key and clicking on the desired tape media in the right pane.

5. From the toolbar, click the **Load Media** button. Or right click on **Media** and choose **Load Media** from the shortcut menu. Or right click on the selected **Media Name** (or the multiple selected names) and choose **Load Media** from the shortcut menu.




5. From the **Media Location** drop-down list, select **Load unknown media** to load a media that is already physically loaded into the Vault's storage device. Select **Load from storage slot** to load a media from a known storage slot within the Vault's storage library.

6. From the **Choose media** drop-down list, select media. It displays all of the media in the storage device.

7. From the **Force Re-Index** drop-down list, use the default setting **Only re-index if needed**. Phoenix RSM indexes the media if necessary, but you can force re-indexing to ensure that your media is re-indexed by selecting **Force a re-Index of media**.

8. Click **OK** to complete the process, and new media appears in the media list.

## Reload Media

As long as you are tracking media, your Vault displays media, even if the media has been unloaded from the storage device. Reloading media means to add it to the storage device after it has been taken offline. If you are using tapes or glass media, insert the media into its storage device. If you are using virtual media, then you do not physically handle the media.

Use the **Reload Selected Media** window to load tape media (such as tapes that are outside of a storage device) into a Vault or to re-index hard disk media. The Reload Selected Media window is almost identical to the Load Media window.

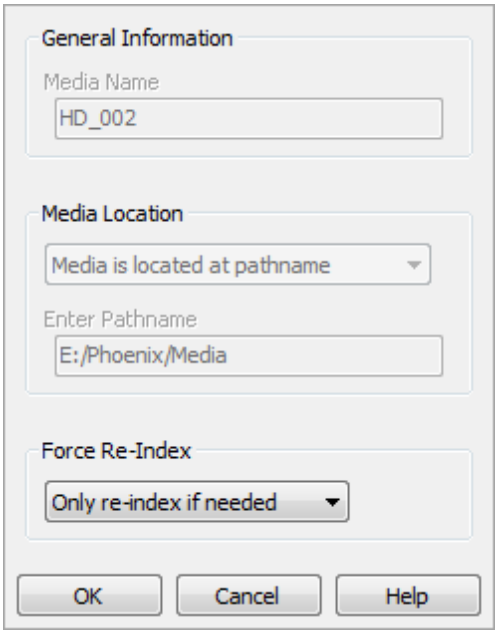
1. From the Vault Admin left pane, click the expand indicator (plus sign) in front of the Vault to reload media to.

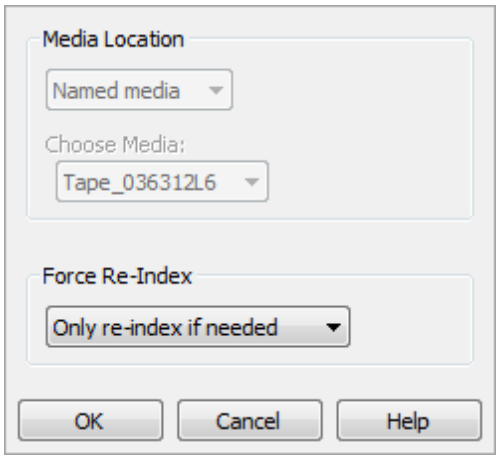
© 2015

2. Click on the expand indicator for **Media** to have a tree of the media names displayed and also to have a list of the media names displayed in the right pane.

3. Select desired media (individual or multiple) then click on the **Load Media** button in the toolbar. Or right-click on the selected media and choose **Reload Media** from the shortcut menu. The **Reload Media** window appears; it looks just like the Load Media window except for the header and the available fields to modify values.

You can reload multiple media by holding the **Shift** key or **Control** key and clicking on the desired media in the right pane.




4. Select a re-indexing option. If the Vault has a good listing of the media in its catalog, select **Only re-index if needed**. The media unit will not be re-indexed if Phoenix RSM determines that re-indexing is not called for. On the other hand, if the catalog entries for the media are suspect or do not exist, the Information Repository will attempt to re-index the media to update its catalog. Select **Force a re-index of media** only if you have a reason to suspect that the catalog on the Vault or the media is incorrect.

5. Click Ok. The media will be reloaded and no longer have a gold bar beneath it.

## Unload Media

The Vault Admin cannot manipulate files (only Data Services can), but the Vault Admin keeps lists of files and media in each Vault, and knows whether or not the media is online, near-line, or offline. By using Unload Media you dictate if files and media are tracked or not tracked when unloading media. In most cases, media is removed when it is full.

Removing media from a Vault can be done in two ways:

© 2015

- **Tracked and managed by the Information Repository -** This is known as unloading to offline status. As long as media is tracked, video or data files remain in the Vault. Although offline, files and metadata are searchable.
- **Not tracked by the Information Repository** - Files are removed from the Vault and are not searchable. If you do not track, you can always reload files and media at a later time.

The process of unloading media is identical for hard disk media and data tape media - with one exception. On data tape media you can either leave the media inside the storage library or remove it from the Information Repository entirely. Standalone data tape drive-based Vaults work the same as data tape library-based Vaults.

## Unloading Media Types

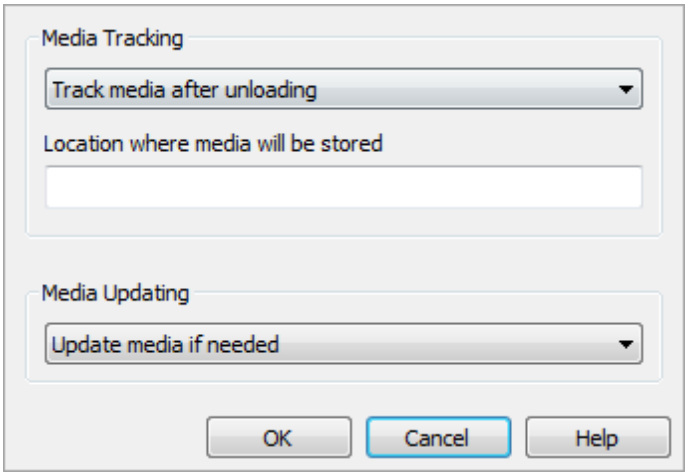
The following subsections instruct you on how to unload a hard disk media and a data tape media.

### Unload Hard Disk Media

1. From the Vault Admin left pane, click the expand indicator (plus sign) in front of the Vault to remove media from.
2. Click on the expand indicator for **Media** to have a tree of the media names displayed and also to have a list of the media names displayed in the right pane.
3. Select desired media (individual or multiple) then click on the **Unload Media** button in the toolbar. Or right-click on the selected media and choose **Unload Media** from the shortcut menu. The **Unload Media** window opens.

You can unload multiple hard disk media by holding the **Shift** key or **Control** key and clicking on the desired hard disk media in the right pane.

4. From the toolbar, click the **Unload Media** button. Or right click on the selected **Media Name** (or the multiple selected names) and choose **Unload Media** from the shortcut menu.




© 2015

5. From the **Media Tracking** drop-down list, select an option:

   **Track media after unloading** - The Vault's memory updates with this information. Should data on this unit of media be required for retrieval, a media request alert (including the **Location where media will be stored**) is displayed by the Information Repository, prompting an administrator to load the required media.

   **Do not track media any longer** - The **Location where media will be stored** text box is disabled. When the media leaves the Information Repository, its entries are removed from the Vault's memory.

6. If you select **Track media after unloading**, type a descriptive note about where media is to be stored in the **Location where media will be stored** text box.

7. From the **Media Updating** drop-down list, select an option:

   **Update media if needed** - The Vault updates the media memory - on the media being unloaded -if it is out of date.

   **Do not update media** - The Vault does not update the media memory for the media being unloaded.

8. Click **OK** to complete the process. The media appears with a gold background in the Vault Admin main window.

Hard disk media is brought back online automatically when available and after 10 minutes has elapsed since it was taken offline. The 10 minutes is to give a user time to unload the media and remove it, if that is what was intended. In cases where the media was automatically taken offline due to technical difficulty (i.e., network outage of SAN or RAID failure), it will come back online automatically within 10 minutes after the technical difficulty has been resolved .

## Unload Tape Media

1. From the Vault Admin left pane, click the expand indicator (plus sign) in front of the Vault to remove media from.

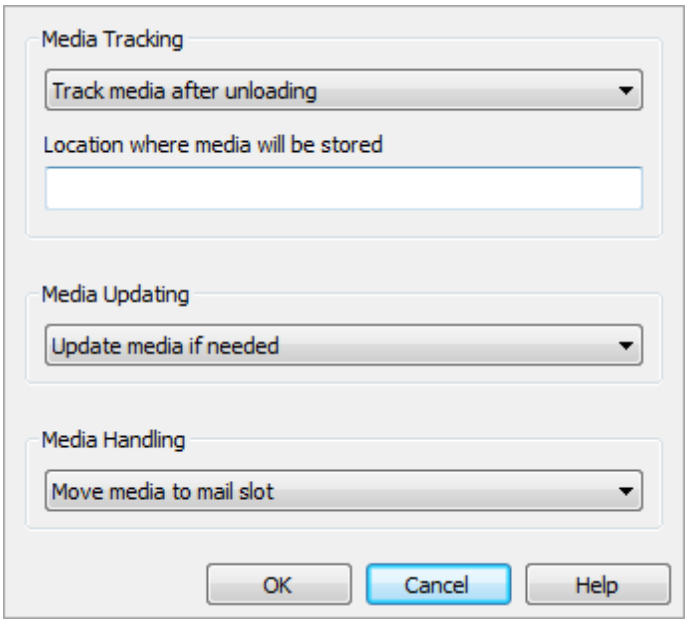
2. Click on **Media** to have a tree of the media names displayed and also to have a list of the media names displayed in the right pane.

3. Select desired media (individual or multiple) then click on the **Unload Media** button in the toolbar. Or right-click on the selected media and choose **Unload Media** from the shortcut menu. The **Unload Media** window opens.

You can unload multiple tape media by holding the **Shift** key or **Control** key and clicking on the desired tape media in the right pane.

4. From the toolbar, click the **Unload Media** button. Or right click on the selected **Media Name** (or the multiple selected names) and choose **Unload Media** from the shortcut menu.

© 2015




5. From the **Media Tracking** drop-down list, select an option:

   **Track media after unloading** - The Vault's memory updates with this information. Should data on this unit of media be required for retrieval, a media request alert (including the **Location where media will be stored**) is displayed by the Information Repository, prompting an administrator to load the required media.

   **Do not track media any longer** - The **Location where media will be stored** text box is disabled. When the media leaves the Information Repository, its entries are removed from the Vault's memory.

6. If you select **Track media after unloading**, type a descriptive note about where media is to be stored in the **Location where media will be stored** text box.

7. From the **Media Updating** drop-down list, select an option:

   **Update media if needed** - The Vault updates the media memory - on the media being unloaded -if it is out of date.

   **Do not update media** - The Vault does not update the media memory for the media being unloaded.

8. From the **Media Handling** drop-down list, select an option:

   **Leave media in library** - The tape will remain in the library after it has been unloaded.

   **Move media to mail slot** - The tape will be moved to the library's mail slot after it has been unloaded.

   When multiple tapes are selected to be unloaded, only the **Leave media in library** option is available.

© 2015

8. Click **OK** to complete the process. The media appears with a gold background in the Vault Admin main window.

## Erase Media

The erase media feature erases data from a unit of media but leaves the media header information intact. Header information comprises the information entered when the media was prepared: media name, owner, rights, and other information. It is better to erase media rather than reformat media whenever possible. When media is erased, an "erased" flag is added that can easily be overwritten.

Erase media:

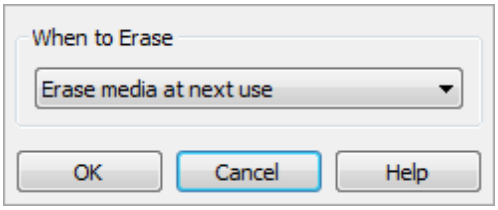
- When physical media with sequential write capabilities (like data tape) is used as the storage media, it must be erased as part of the purge process. If it is part of a multi-level storage hierarchy where files are migrated and replicated, viable data on the media must be moved to other media and the original media erased in order to purge old, expired data.
- When media is used in a cycled Information Repository. At the end of a cycle, the old media being reintroduced needs to be erased by the Information Repository before it can be reused.

To erase media:

1. From the Vault Admin left pane, click the expand indicator (plus sign) in front of the Vault to erase media from.
2. Click on the expand indicator for **Media** to have a tree of the media names displayed and also to have a list of the media names displayed in the right pane.
3. Select desired media (individual or multiple) then click on the **Erase Media** button in the toolbar. Or right-click on the selected media and choose **Erase Media** from the shortcut menu. The **Erase Media** window opens.

You can erase multiple media by holding the **Shift** key or **Control** key and clicking on the desired media in the right pane.

4. From the toolbar, click the **Erase Media** button.Or right click on the selected **Media Name** (or the multiple selected names) and choose **Erase Media** from the shortcut menu.




5. From the **When to Erase** drop-down list, select an option:

   **Erase media at next use** - The media is erased just prior to the next time it is used in a job.

   **Erase media now** - The media is loaded into a drive and erased immediately.

© 2015

6. Click the **OK** button to activate your selection.

## Start Vaults Manually

When managing an Information Repository, there may be times when Vaults do not start automatically, so you need to start them manually. **Vault Service** is used to start a vault manually. See Manage Services for information on manually controlling **Vault Service**.

## Vault Details

All the active Vaults within the Information Repository are displayed under Entire Network in the left pane of the Vault Admin window.

- Click the expand indicator (plus sign) in front of a Vault to view the sub-items associated with the Vault and to activate toolbar buttons. Certain icons in the toolbar are only active when a Vault, Media, or Drive is selected.

The following are details to view:

- Information

- Current Clients

- Volumes (displayed only in advanced mode, from the Vault Admin main menu click **View** > **Enable Advanced**)

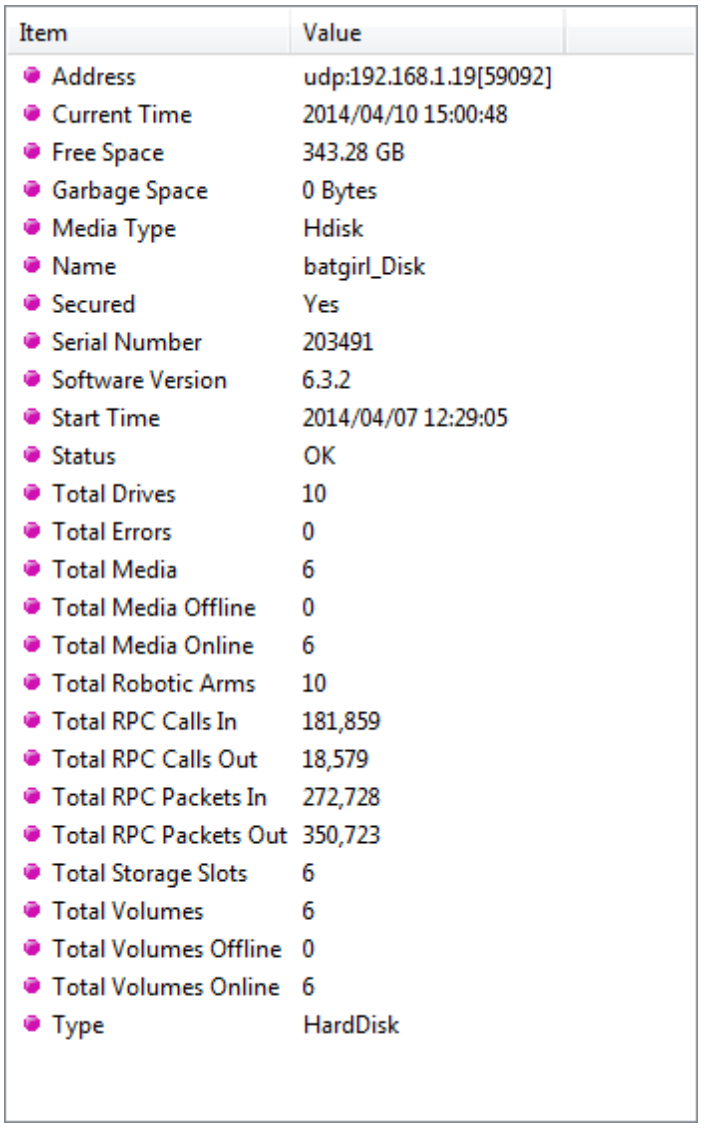
- Media (depending on media type, displayed information varies)

- Drives (depending on media type, displayed information varies)

### Information

From the Vault Admin left pane, selecting **Information** displays the overall details of the Vault in the Vault Admin right pane.

© 2015



| Item | Value |
|---|---|
| Address | udp:192.168.1.19[59092] |
| Current Time | 2014/04/10 15:00:48 |
| Free Space | 343.28 GB |
| Garbage Space | 0 Bytes |
| Media Type | Hdisk |
| Name | batgirl_Disk |
| Secured | Yes |
| Serial Number | 203491 |
| Software Version | 6.3.2 |
| Start Time | 2014/04/07 12:29:05 |
| Status | OK |
| Total Drives | 10 |
| Total Errors | 0 |
| Total Media | 6 |
| Total Media Offline | 0 |
| Total Media Online | 6 |
| Total Robotic Arms | 10 |
| Total RPC Calls In | 181,859 |
| Total RPC Calls Out | 18,579 |
| Total RPC Packets In | 272,728 |
| Total RPC Packets Out | 350,723 |
| Total Storage Slots | 6 |
| Total Volumes | 6 |
| Total Volumes Offline | 0 |
| Total Volumes Online | 6 |
| Type | HardDisk |

The following are the items listed:

**Address**: The network address of the Vault selected and the Vault's port number.

**Current Time**: The Vault's internal clock time. This is mapped to the Vault's host computer.

**Free Space**: The amount of free space available in the Vault.

**Garbage Space**: The amount of purge space in the Vault (typically zero on hard disk based Vaults).

**Media Type**: Additional information about the storage device technology used by the Vault. (Hard disk based Vaults always have a Media Type of Hdisk while data tape based Vaults list the type of technology used, such as DLT or LTO.)

**Name**: The name of the Vault selected.

**Secured**: Security of Vault; secured or unsecured.

© 2015

**Serial Number**: A number created at the time of manufacture mapping to a license.

**Software Version**: The version of software used by the Vault.

**Start Time**: The date and time of the Vault's last startup cycle.

**Status**: The status of the Vault regarding errors or media requests.

**Total Drives**: The total number of storage media drives within the Vault's storage device.

Hard disk Vaults are mapped differently than other Vault storage devices. Vault's mapped at a physical drive may be one-to-one or virtualized making the ratio higher or lower.

**Total Errors**: A cumulative list of errors since the Vault has been online. This number is reset whenever the Vault is restarted.

**Total Media**: The amount of media, online and offline, being tracked and managed by the Vault.

**Total Media Offline**: Includes formatted media outside of the Vault's storage that is tracked by the Information Repository.

**Total Media Online**: Includes formatted media within the Vault's storage that is tracked by the Information Repository.

**Total Robotic Arms**: The number of robotic devices within the Vault's storage used to move media from storage slots to drives and back again. Hard disk based Vaults usually have as many robotic arms as drives. Other storage devices, like data tape based devices, usually have only one robotic arm.

**Total RPC Calls In**: The number of remote procedural calls that have been made to the Vault since its latest startup cycle.

**Total RPC Calls Out**: The number of remote procedural calls made by the Vault since its latest startup cycle.

**Total RPC Packets In**: The number of network packets that have been received by the Vault since its latest startup cycle.

**Total RPC Packets Out**: The number of network packets that have been sent by the Vault since its latest startup cycle.

**Total Storage Slots**: Storage slots are areas where media is stored in the Vault's storage when it is not in a media drive. With data tape and other physical media-based storage devices, the total storage slots number is fixed by the storage device. In hard disk Vaults the number is usually mapped to the number of virtual media units set up in the Vault.

**Total Volumes**: The number of volumes on media being tracked and managed by the Vault. It includes all online and offline media tracked.

**Total Volumes Offline**: Includes volumes on formatted media outside the Vault's storage tracked by the Information Repository.

**Total Volumes Online**: Includes volumes on formatted media within the Vault's storage tracked by the Information Repository.

© 2015

**Type**: The storage device technology the Vault uses.

## Current Clients

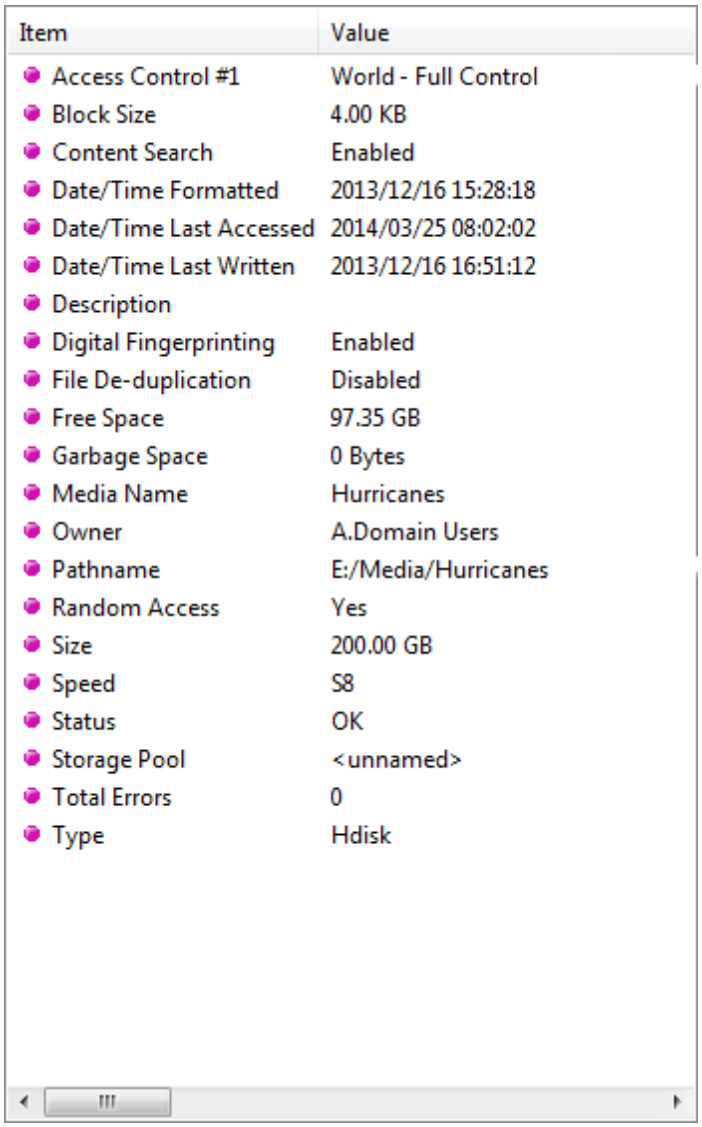
From the Vault Admin left pane, selecting **Current Clients** displays details in the Vault Admin right pane about computers on which the Information Repository is currently working. A good way to watch for activity is to monitor Network Activity.

- Click **Current Clients**, and if there is any current working activity, the computers are listed in the Vault Admin right pane. You can opt to change the format of computer details listed from the **Options** menu > **Address Format**.

## Media

From the Vault Admin left pane, selecting **Media** displays a list of the media for the selected Vault. Then, select a specific piece of media from the left pane, and the details of that unit of media display in the Vault Admin right pane.

© 2015



| Item | Value |
|---|---|
| Access Control #1 | World - Full Control |
| Block Size | 4.00 KB |
| Content Search | Enabled |
| Date/Time Formatted | 2013/12/16 15:28:18 |
| Date/Time Last Accessed | 2014/03/25 08:02:02 |
| Date/Time Last Written | 2013/12/16 16:51:12 |
| Description | |
| Digital Fingerprinting | Enabled |
| File De-duplication | Disabled |
| Free Space | 97.35 GB |
| Garbage Space | 0 Bytes |
| Media Name | Hurricanes |
| Owner | A.Domain Users |
| Pathname | E:/Media/Hurricanes |
| Random Access | Yes |
| Size | 200.00 GB |
| Speed | S8 |
| Status | OK |
| Storage Pool | <unnamed> |
| Total Errors | 0 |
| Type | Hdisk |

**Access Control #1**: The first of sixteen controls that can be assigned to the selected media. Each object in a system, like files or directories, has a security attribute identifying it to the access control list (ACL) telling the operating system of access rights each user has to an object.

**Barcode/ID** (data tape media only): The barcode number or label assigned to the media selected. (If the storage device has a barcode reader, the data is assigned by the physical barcode label on the media, and any other information is ignored by the Information Repository.)

**Block Size**: The block size used by the media unit selected.

**Content Search**: Indicates if content search is enabled.

**Current Location** (data tape media only): The current location of the media.

**Date/Time Formatted**: The most recent time the media unit was formatted for use.

© 2015

**Date/Time Last Accessed**: The last time the media unit was accessed for use by the Information Repository.

**Date/Time Last Written**: The last time data was written to the selected media.

**Description**: The description from the Prepare Media dialog box.

**Digital Fingerprinting**: Indicates if digital fingerprinting is enabled.

**File De-duplication**: Indicates if de-duplication is enabled.

**Free Space**: The available amount of space on the media for use.

**Garbage Space**: The amount of used media space that is eligible to be purged from the Information Repository.

**Home Location** (data tape media only): The assigned media slot in a drive.

**Media Name**: The name of the media selected. The name is part of the media label.

**Owner**: Displays the user logged into the Information Repository during media format.

**Pathname** (hard disk and shadow hard disk media only): The directory path of where the media's space actually resides.

**Random Access**: Indicates if random access of the media is permitted.

**Size**: The capacity of the media unit selected.

**Speed**: A performance rating where different types of media are rated by access and read/write performance. Hard disk is considered the highest performance media and DDS-2 data tape is a lower performing media.

**Status**: The overall health and usability of the media.

**Storage Pool**: The name of the storage pool, if the media belongs to one.

**Total Errors**: The number of errors the selected media has generated.

**Total Volume**: (advanced mode only): The number of volume the media holds.

**Total Loads** (data tape media only): The number of times the selected media has been loaded into a drive.

**Type**: The storage device used by the media (hard disk, data tape, etc.)

**Volume #** (advanced mode only): Lists each volume associated with the media.

## Volumes

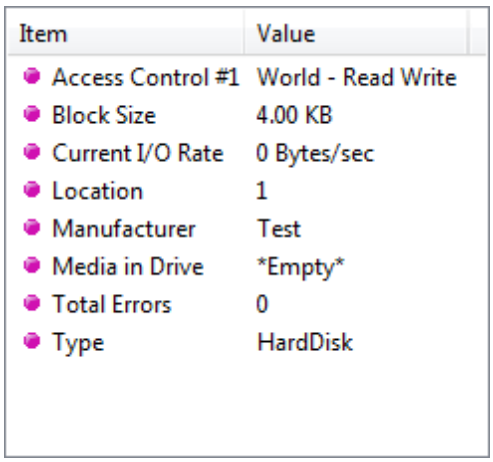
From the Vault Admin left pane, selecting **Volumes** displays volume information on the media if the media has more than one volume associated with it for the selected Vault. A data tape might store data on both sides of the tape, presenting two volumes of media storage. Select a specific volume from the left pane, and the details about that volume display in the Vault Admin right pane.

© 2015

Only displays if in advanced mode. From the Vault Admin main menu click **View** > **Enable Advanced**.

### Drives

From the Vault Admin left pane, selecting **Drives** displays a list of drives in the Vault. Then, select a specific drive from the left pane, and the details about that drive display in the Vault Admin right pane.




**Access Control #1**: The first of sixteen controls that can be assigned to the selected media.

**Block Size**: The block size employed by the media when it is accepting data.

**Current I/O Rate**: The rate at which data is being written to media.

**Last Cleaning** (data tape media only): The last time the media has been physically cleaned.

**Location**: The slot number in the drive that the media occupies.

**Manufacturer**: The name of the company that manufactured the drive.

**Media in Drive**: The media's assigned name.

**Total Errors**: The number of errors a unit of media unit has generated.

**Total Loads** (data tape media only): The total number of times a unit of media has been physically loaded into the drive.

**Type**: The type of drive.

## Network Activity

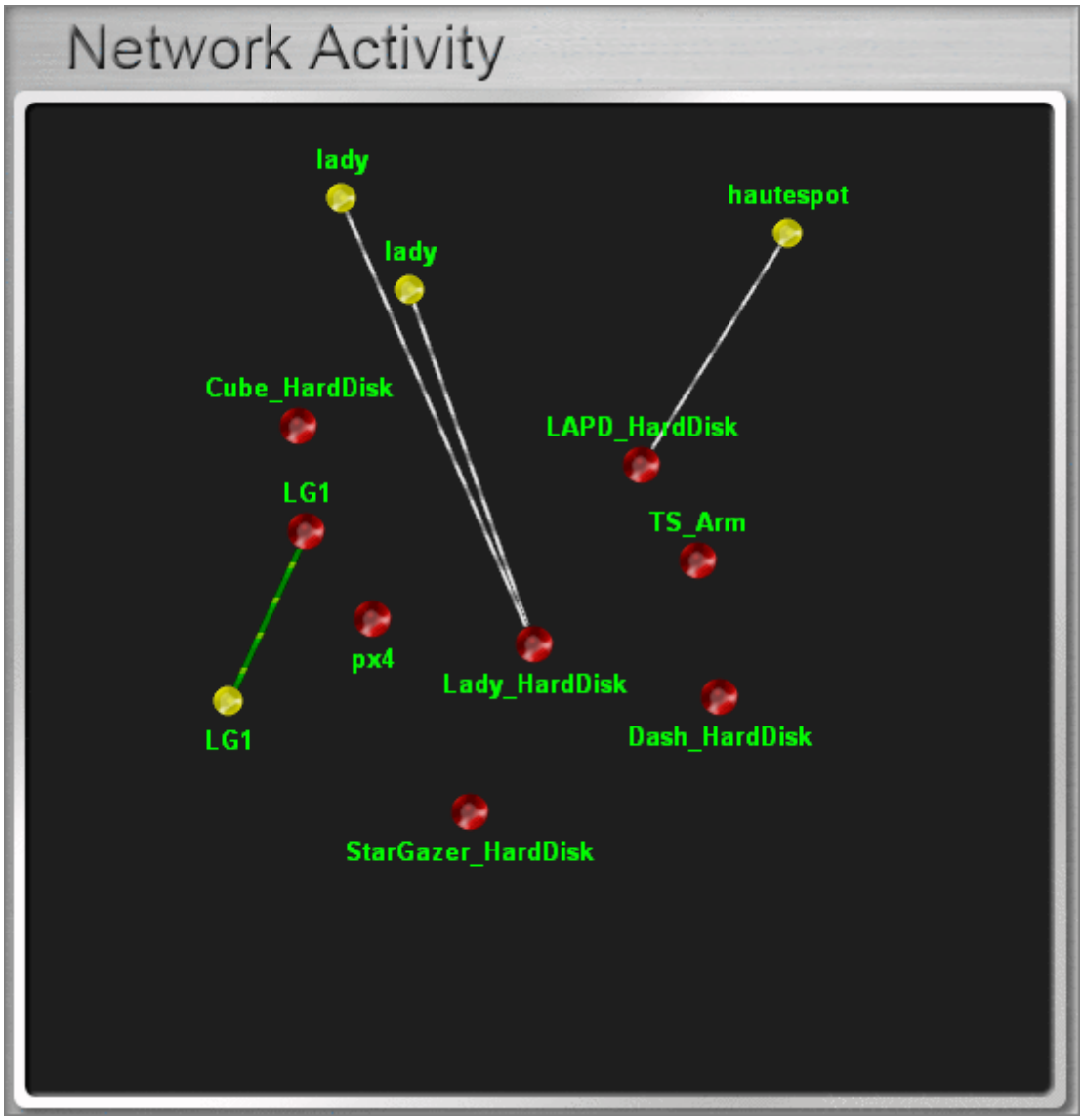
Network Activity graphically represents, in real-time, each client and Vault on the network. It works together with the Vault Stats and Mini Vault Stats windows to monitor all data, media, and Vault operations within the Information Repository.

© 2015

Remember that a Vault is a storage device used to store files. The Vault drives the storage device and provides memory resources for program execution, metadata management, and continuous monitoring.

From your suite of product applications, open the Network Activity application (NetActivity.exe). From Network Activity access Mini Vault Stats to see high level Vault activity information. Or access Vault Stats to view detailed vault activity information.

Every client and Vault in the Information Repository is represented by a sphere and a label in the Network Activity window. Clients appear when jobs are running and the activity is denoted by dynamic lines connecting clients and Vaults. As a job is running, move the mouse pointer over the client symbol to view Job, User, and Status details. If you need to freeze the current display of Network Activity, right-click and hold the application's **Title** bar.




© 2015

### Network Activity Menu Items

| Menu Items | Description |
|---|---|
| **File > Exit** | Close the application |
| **Advanced > Update Fast** | Increase the Network Activity screen update rate. |
| **Advanced > Force Vault Lookup** | Force a display update of Vaults active on the network. |
| **Advanced > Vault Expire Fast** | Clear the screen of inactive Vaults. |
| **Advanced > Client Expire Fast** | Clear the screen of inactive clients. |
| **Help > Current Page** | Open online help to the Network Activity page. |
| **Help > Network Activity Overview** | Open online help with focus on Network Activity. |
| **Help > Contents** | Open the local version of online help. |
| **Help > Online Help** | Open the web-based version of online help. |
| **Help > /technical Support** | Open the support webpage. |
| **Help > About Network Activity** | Open the About Network Activity window. |

## Network Activity Symbols

Network Activity generates and places Vault symbols randomly on the window, but you can move the Vault symbols. In addition, from the Network Activity **Advanced** menu, you can modify the mode as to how the Network Activity window updates.

1. Move the mouse pointer over the Vault symbol.
2. Click and drag the Vault symbol to another location within the window.

To open Mini Vault Stats or Vault Stats move the mouse pointer over the a Vault label or symbol and right-click for the shortcut menu.

To quickly open Mini Vault Stats, double-click a Vault label or symbol.

© 2015

There are many different Network Activity symbols that can display on screen. The following list identifies the symbols you may see:

- **Red circle** - A Vault in the Information Repository.
- **Yellow circle** - A client in the Information Repository.
- **Red line, pulsing** - The Information Repository is waiting for offline media and operator intervention is required.
- **White line, pulsing** - This is normal activity showing the Information Repository is waiting for a connection slot.
- **Green line, pulsing** - The client is waiting for a unit of media to be moved into a drive. This is common with data tape and optical libraries.
- **White line, stationary** - A client connection is idle, waiting for resources.
- **Blue line, stationary** - The client status is unknown.
- **Green line, moving** - The Information Repository is transferring data; the line direction indicates the way data is moving.
- **Blue line, moving** - A media operation is in progress; load, unload, prepare, erase, etc.

## Mini Vault Stats

Mini Vault Stats provides a high level perspective of Vault activity through a graphical display of Vault performance when data is transferred from clients or between Vaults on the network.

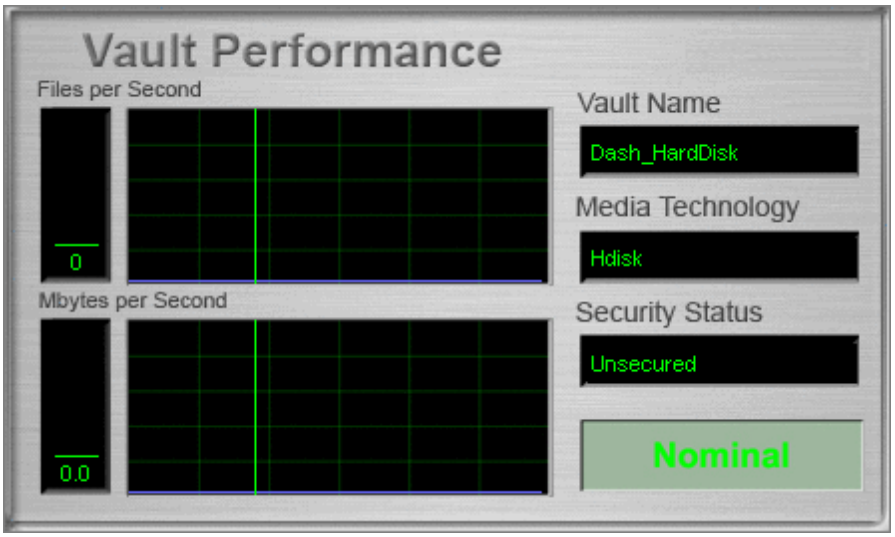
To access Mini Vault Stats:

- From Network Activity double-click a Vault label or symbol.

Or,

1. From Network Activity, move the mouse pointer over a Vault symbol, and right-click.
2. From the shortcut menu, select **Mini Vault Stats**.

© 2015




On the Mini Vault Stats window the **Files per Second** monitors performance of data transfer between Vaults and the **Mbytes per Second** displays data transfer from clients.

The display at the bottom right of the Mini Vault Stats window, shows Nominal, Media Request, or Trouble.

- **Nominal** - Everything is okay.
- **Media Request** - Request for offline media to be reloaded.
- **Trouble** - Indicates a serious problem.

### Mini Vault Stats Menu Items

| Menu Items | Description |
|---|---|
| **File > Exit** | Close the application. |
| **Help > Current Page** | Open online help to the Mini Vault Stats webpage. |
| **Help > Mini Vault Stats Overview** | Open online help with focus on Mini Vault Stats. |
| **Help > Contents** | Open the local version of online help. |
| **Help > Online Help** | Open the web-based version of online help. |
| **Help > Online Support** | Open Technical Support webpage. |
| **Help > About Mini Vault Stats** | Open the About Mini Vault Stats window. |

© 2015

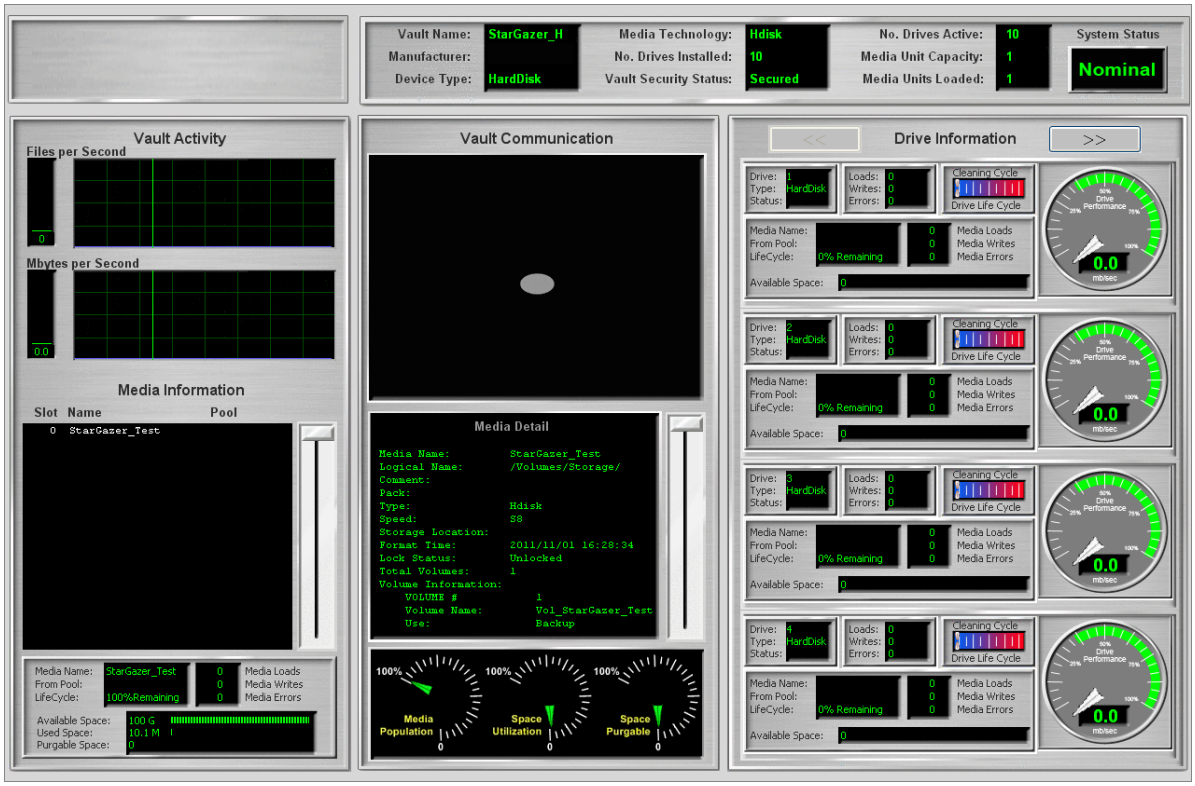
## Vault Stats

Use Vault Stats to gain a detailed perspective of individual Vault activity on the network. One or multiple Vault Stats can be open at a time. Vault Stats provides perspective for daily management and troubleshooting issues that may arise on the network.

To access Vault Stats:

1. From Network Activity, move the mouse pointer over a Vault symbol, and right-click.
2. From the shortcut menu, select **Vault Stats**.

Vault Stats requires a minimum screen resolution of 1280 x 1024.




### Vault Stats Menu Items

| Menu Items | Description |
|---|---|
| **File > Exit** | Close the application. |
| **Help > Current Page** | Open online help to the Vault Stats webpage. |
| **Help > Vault Stats Overview** | Open online help with focus on Vault Stats. |

© 2015

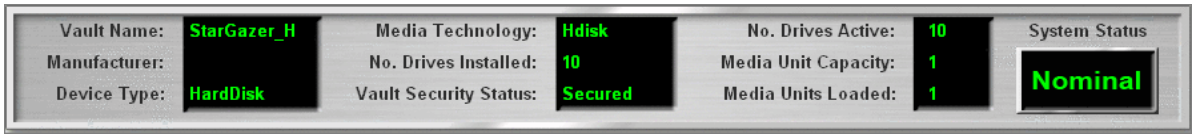
| Menu Items | Description |
|---|---|
| **Help > Contents** | Open the local version of online help. |
| **Help > Online Help** | Open the web-based version of online help. |
| **Help > Online Support** | Open Technical Support webpage. |
| **Help > About Vault Stats** | Open the About Vault Stats window. |

## Vault Stats Anatomy

Vault Stats displays elements to monitor such as Vault information, performance, communication, and drive and media information. The following describes each pane within the Vault Stats window:

### Vault Configuration bar

Located in the Vault Stats upper-right part of the window, the Configuration bar displays information about the Vault's identity and capabilities based on the media resources available to it.




Some of the details in the pane include Vault name, manufacturer, device type, security level applied to Vault, number of drives, and media information.

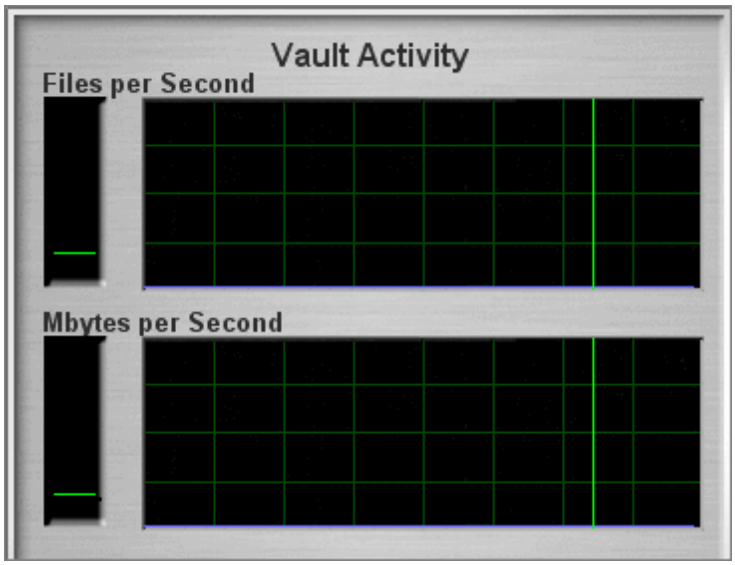
The System Status can be Nominal, Media Request, or Trouble, and switches between the three depending on actual status.

- **Nominal** - Everything is okay.
- **Media Request** - Request for offline media to be reloaded.
- **Trouble** - Indicates a serious problem.

### Vault Activity pane

Located in the Vault Stats upper-left part of the window, the Vault activity pane displays the overall performance in files per second and megabytes per second.

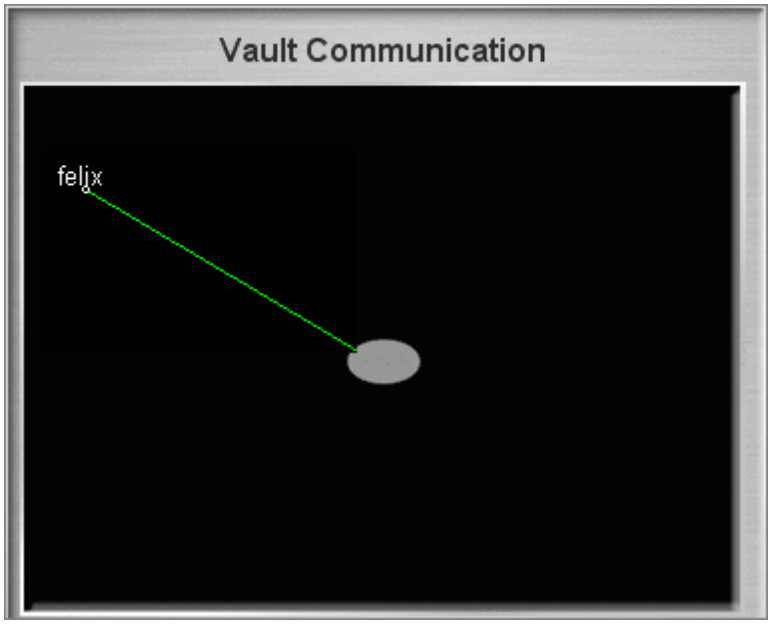
© 2015




- **Files per Second** - Monitors performance of data transfer to and from Vaults.
- **Mbytes per Second** - Displays data transfer performance from clients or Vaults.

### Vault Communication pane

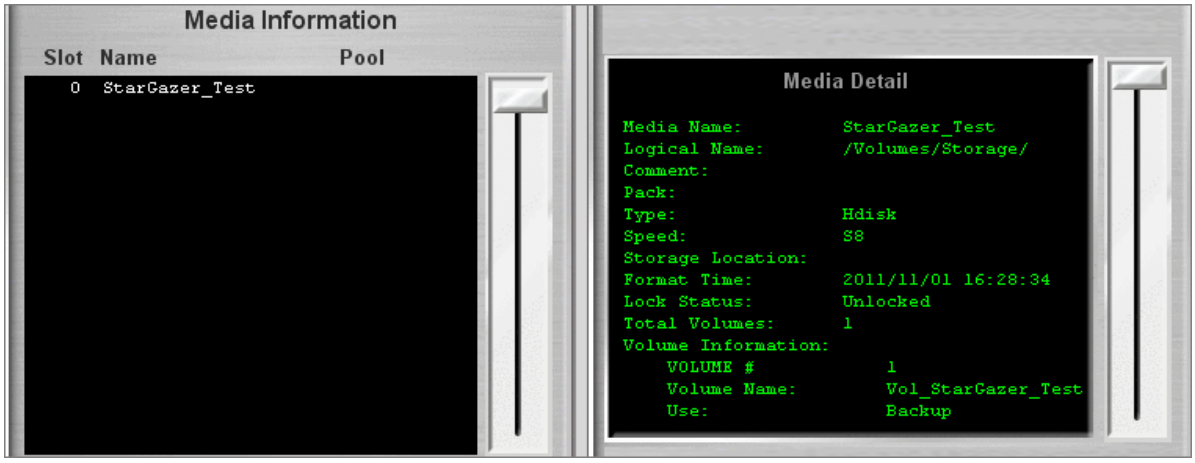
Located in the Vault Stats upper-middle part of the window, the Vault communication pane displays connection activity. Connections can be between clients engaged in job activity, or connections to other Vaults during data migration or replication activity. Connection types are color coded to define different activities. See Network Activity Symbols.




### Media Information panes

© 2015

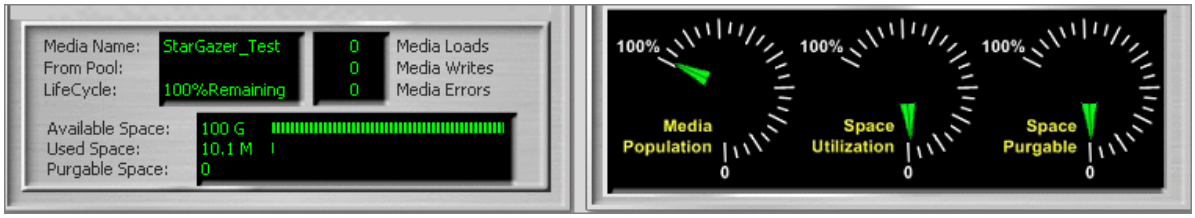
Located in the Vault Stats mid-section of the window, the media information panes include a list of media available in the Vault and then the media detail.




- From the media information pane, select a unit of media. The corresponding set of information about the media unit displays in the media detail pane.

## Vault Statistics and Vault Space dials

Located in the Vault Stats lower-left part of the window, the Vault statistics and Vault space panes provide details about media in Vaults.




The left pane displays the Vault media statistics, and the right pane displays Vault space dials - each meaning the following:

- **Left dial** - Displays the percentage of the media population capacity used. It compares the amount of media loaded in the Information Repository to the amount of media that can be loaded into the Vault. For example, if a data tape library-based Vault can hold ten data tapes and has only eight loaded, the dial would indicate an 80% media population. If using hard disk Vaults, the dial would be a 100% all the time.

- **Middle dial** - Displays the overall Vault space used by stored and managed files. A dial reading of 100% would mean there is no space available.

© 2015

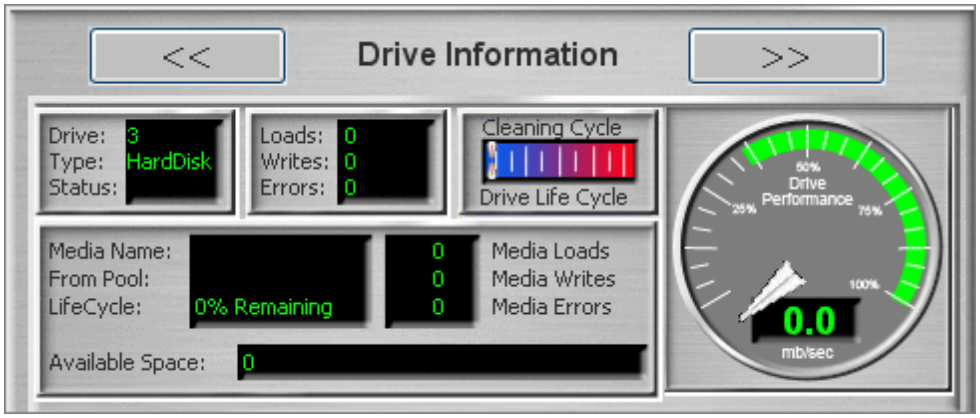
- **Right dial** - Displays how much unneeded data is on a Vault waiting to be purged. This indicator is typically used with sequential write media formats, such as data tape. Media with non-sequential formats, such as hard disk, usually purge files immediately when a purge cycle starts. The purge files then make room for added space to the Information Repository. Data tape media requires files to be copied to other media units while reformatting the original media to complete a purge cycle. In this case, the dial would indicate how much space could be made available through the purge cycle operation.

## Drive Information

Located in the Vault Stats right part of the window, each drive information pane is determined in the following way:

- **Data Tape** - One drive information pane displays for every drive in the data tape library.
- **Hard Disk** - One drive information pane displays for each data stream connection. The data stream limitations are set in Vault Admin Properties, in the **Device** tab, **Connection Resources** group. The data stream connections determine how many sessions can be running at any one time in a Vault. Setting data stream connections can help limit usage so the network does not get saturated.

Up to four drive panes can be displayed concurrently, but additional drive panes can be displayed by clicking the **Previous** or **Next** buttons. The drive information stack rotates up or down, one pane for each button click.




Each drive pane has three basic parts:

- **Top part** - Displays drive information of name or number, the media technology it is based on, its use and problem history, and drive cleaning and life cycle information.
- **Bottom part** - Displays information about the media the drive is using. This is the same information provided in the Vault statistics pane.
- **Right part** - Displays the drive performance, and read or write speed in near real-time. For data tape drive, the dial specifically shows the I/O (input/output) transfer rate throughout the drive. For hard disk, the dial shows data streaming usage.

© 2015

# Remove Vaults

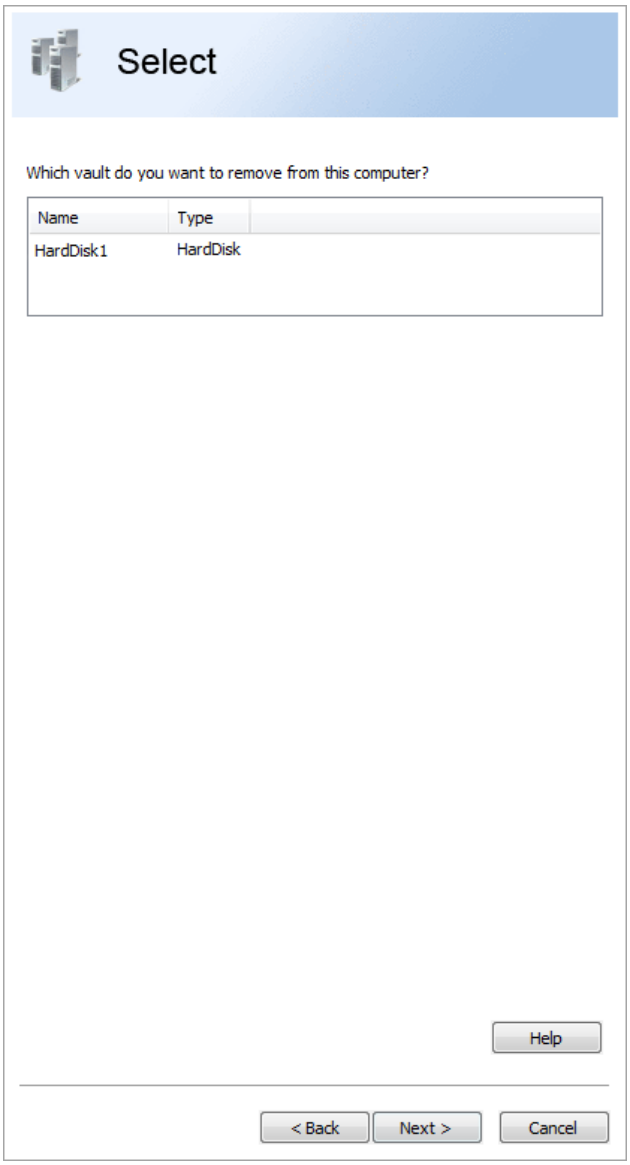
Use the Phoenix RSM Add or Remove Vault Wizard to remove hard disk based Vaults, tape library Vaults, and single tape drive Vaults from your Information Repository. Removing a Vault is easy. All you have to do is remove the Vault using the wizard and then reboot the computer where you have removed the Vault.

When you remove a Vault, the data in the Vault is not erased and your license file is not affected.

## Removing a Vault

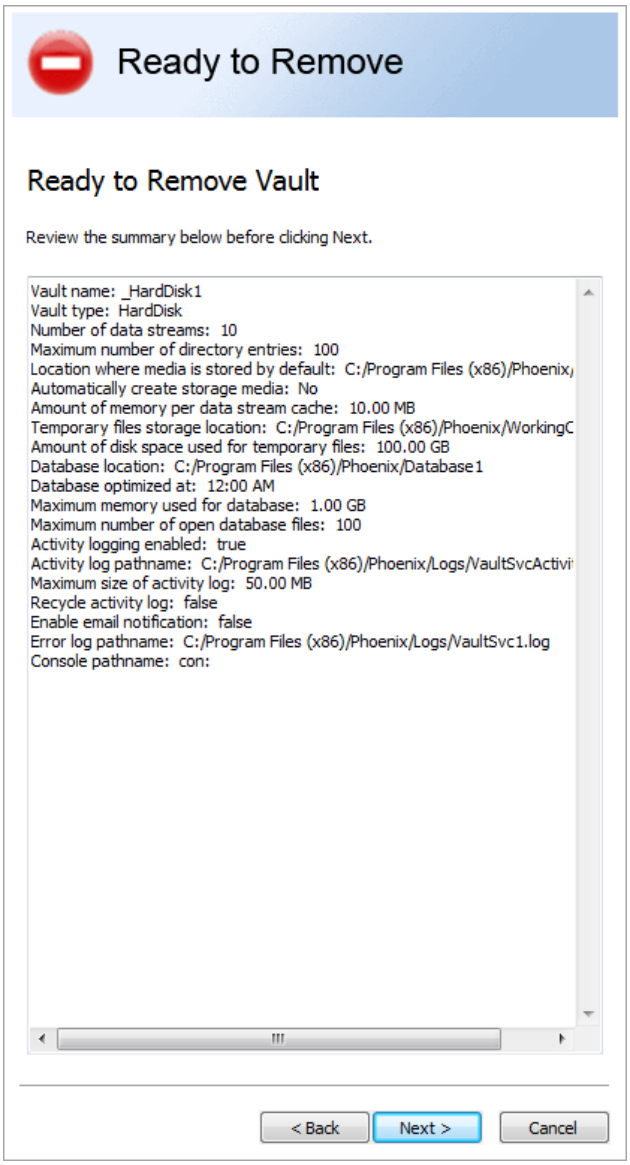
1. From your suite of product applications, open the Add or Remove Vault Wizard application (AddRemVltWzrd.exe). The Welcome window appears. For complete descriptions of the wizard buttons and windows refer to Add or Remove Vault Wizard.
2. Click **Next**, for the Add or Remove window.
3. Select **Remove an existing Vault from this computer**.
4. Select **Next** for the Select window.

© 2015




5. Select the Vault you want to remove.
6. Click **Next** for the Ready to Remove window.

© 2015

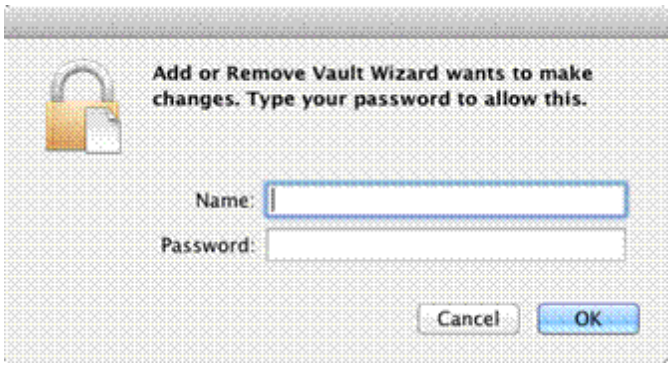

Ready to Remove
Ready to Remove Vault
Review the summary below before clicking Next.
Vault name: _HardDisk1
Vault type: HardDisk
Number of data streams: 10
Maximum number of directory entries: 100
Location where media is stored by default: C:/Program Files (x86)/Phoenix/
Automatically create storage media: No
Amount of memory per data stream cache: 10.00 MB
Temporary files storage location: C:/Program Files (x86)/Phoenix/WorkingC
Amount of disk space used for temporary files: 100.00 GB
Database location: C:/Program Files (x86)/Phoenix/Database1
Database optimized at: 12:00 AM
Maximum memory used for database: 1.00 GB
Maximum number of open database files: 100
Activity logging enabled: true
Activity log pathname: C:/Program Files (x86)/Phoenix/Logs/VaultSvcActivi
Maximum size of activity log: 50.00 MB
Recycle activity log: false
Enable email notification: false
Error log pathname: C:/Program Files (x86)/Phoenix/Logs/VaultSvc1.log
Console pathname: con:
< Back
Next >
Cancel

7. Review the displayed summary for the correct Vault information.

8. When ready to remove the Vault, click **Next**.

    - Mac users will be prompted for an Administrator Name and Password. The Name field may already be populated with the name of the user running the Vault Wizard.

© 2015




- After entering a Name and Password, click **OK**. The Vault will stop immediately.

A restart is not required on a Mac.

9. In the Completed window, click **Finish** to exit the Add or Remove Vault Wizard.

10. Restart your computer, or to remove another Vault or add a Vault, open the Add or Remove Vault Wizard again. See Adding a Vault.

# Camera Management

The camera component is the most important for any video surveillance solution. Not only does SoleraTec's Phoenix RSM effortlessly connect to any RTSP-enabled IP camera or VMS-managed cameras, but it also fully manages any number of storage devices for all of your accumulated video assets. While recording and capturing your video, you can monitor live video feeds using the Live Viewer application - featuring an unlimited live video matrix with the ability to view 16 channels at a time.

This camera management chapter encompasses the tools used for recording and capturing video feeds:

**Add Camera Wizard** - As part of the Camera Policies application, use the Add Camera Wizard to easily add a camera and a camera (or recording) policy. All you need to do is follow the wizard steps to begin recording video.

**Camera Policies** - Use the Camera Policies application to configure RTSP-enabled IP cameras or VMS-managed cameras and create recording policies to capture video into your Vaults. Once inside the Information Repository, take advantage of your product's full management capabilities such as migrating, replicating, searching, and archiving video assets.

**Record** - Record live video feeds from any RTSP-enabled IP camera directly into the Information Repository. Remember that RTSP stands for Real Time Streaming Protocol, to control streaming media servers. For a list of RTSP URLs for IP cameras, go to http://www.SoleraTec.com/support/rtsp/rtsp_listing.

**Capture** - Capture video from cameras controlled by a VMS (Video Management System such as Milestone, OnSSI, or exacqVision) into the Information Repository.

© 2015

**Camera Configurations** - Use Camera Configurations to manually add cameras to your Information Repository and to configure them. If you plan to capture video from a VMS, you must use the Camera Configurations window - not the Add Camera Wizard - in order to set up a policy to grab video from the VMS.

**Motion Detection** - If motion detection information is provided by your RTSP-enabled IP camera, and if Phoenix RSM supports collecting that the information, then camera settings are set to preserve motion metadata along with captured video.

Once videos have been captured into the Information Repository, Data Service Policies can manage your data assets from the Vault(s) within the Information Repository. This provides for an efficient and powerful multi-tiered Information Repository. Find out other benefits to your solution by reading about **Load Balancing** or **Complete and Accurate Stored Files** in Data Management. See also Live Viewer.

### Workflow - Basic Camera Steps

1. From your suite of product applications, open the Camera Policies application (CameraPolicies.exe). For further explanation of how to launch applications using different operating systems, see Getting Started.
2. Add a camera and a camera policy to your solution. The easiest and quickest way to do this is through the Add Camera Wizard. When adding a camera through the Add Camera Wizard, a recording policy is automatically created for the camera. From the Camera Policies main menu, select **Tools** > **Add Camera Wizard**.
    - Instead of using the Add Camera Wizard, you could add a camera manually through Camera Configurations, and then create a recording policy separately. See Create a Policy.
    - You can always modify or delete a Camera Policy once it has been created. See Modify a Policy and Delete a Policy.
    - The Add Camera Wizard provides only **Standard** mode options.
3. Define when to record videos from the RTSP and VMS-managed camera using Camera Policies **Scheduling** tab.
4. (Optional) Set Camera Policies from **Standard** mode to **Advanced** mode, select from the **View** menu > **Enable Advanced mode**. This provides more options for direct connect IP cameras (video processing, Vault storage, and performance and log file options). See Advanced Mode.
5. (Optional) Save, restore, or copy Camera Policies using the import and export camera configuration options. From the Camera Configurations main menu, select **File** > **Import from** or **Export to**.

Once your camera is set up and recording, see Live Viewer and learn how to view the video streams.

## Add Camera Wizard

Adding a camera to your video surveillance solution is essential. You can do this a couple of different ways with SoleraTec's Phoenix RSM, but the fastest and simplest way is by using the Add Camera Wizard.

© 2015

The camera wizard not only guides you through how to add an RTSP-enabled IP camera, but it also automatically creates a camera (or recording) policy to accompany the camera. The Recording policy designates how to store recorded video from your camera into the Information Repository.

Do not use the Add Camera Wizard if:

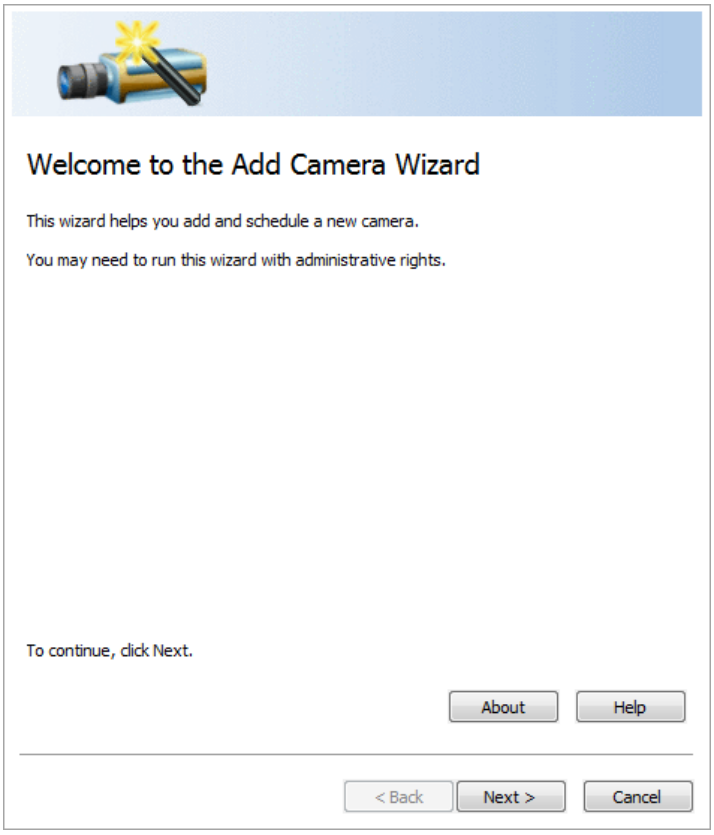
- You are capturing video from VMS-managed cameras (Video Management System such as Milestone, OnSSI, or exacqVision). Instead, manually add your cameras using Camera Configurations.
- The extended metadata file (MetadataExtensions.cfg) is in use.

## Adding a camera and recording video setup

1. From your suite of product applications, open the Camera Policies application (CameraPolicies.exe).

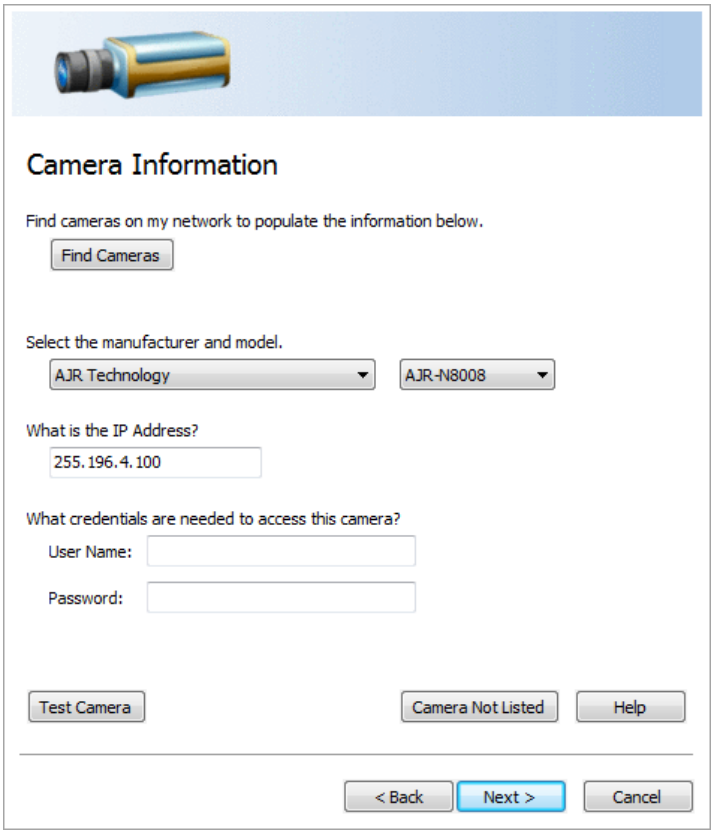
   From the Camera Policies toolbar, click the Wizard button. The Welcome window appears. Each wizard dialog box includes **Back**, **Next**, **Help**, and **Cancel** buttons. The **Back** button navigates you back to the previous dialog box (except on the Welcome window), and the **Next** button accepts current values and advances you to the next window in the wizard. The **Help** button opens documentation, and the **Cancel** button closes the wizard without saving values.

   The **About** button appears on the first wizard window to provide information, and the **Finish** button appears on the last wizard window to complete the process.


Welcome to the Add Camera Wizard
This wizard helps you add and schedule a new camera.
You may need to run this wizard with administrative rights.
To continue, click Next.
About
Help
< Back
Next >
Cancel

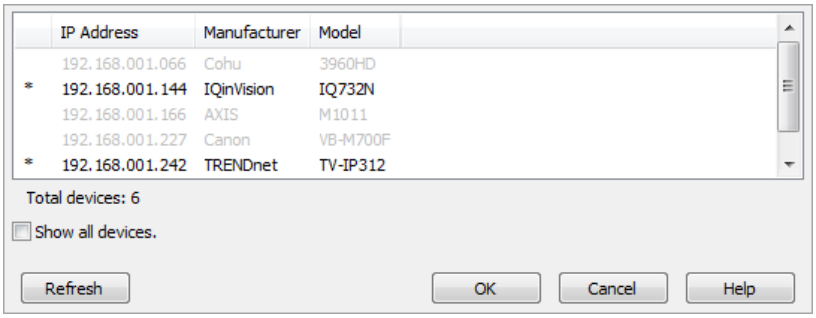
© 2015

2. Click **Next** for the Camera Information window.




3. To add camera information, either click the **Find Cameras** button or select the camera from the **Select the manufacturer and model** drop-down lists.

   If you click the **Find Cameras** button a Search Results window appears showing a list of cameras found on the network. If your camera is not on the list, select the **Show all devices** checkbox for any additional cameras on the network and other devices to display. If your camera still does not display, use the **Select the Manufacturer and model** drop-down lists option and type the IP address, or you can add it manually in Camera Configurations. In the Search Results window, cameras in use appear grayed-out and available cameras for configuration have an asterisk (*) in the first column. Select a camera and click **OK**, or double-click the camera item for the camera information to configure.




© 2015

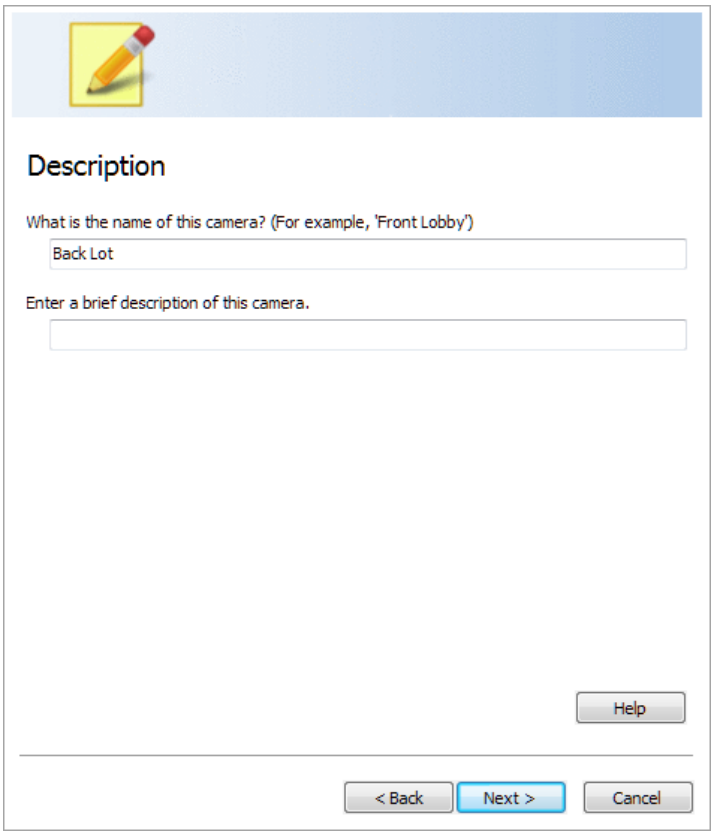
If the camera manufacturer or model is not listed, use the Camera Configuration window to add the camera rather than this wizard.

4. In the **What is the IP Address?** text box, type the host name or IP address in dot notation.
5. Type the **User Name** and **Password** for the camera if they are required to access it.
6. Click the **Test Camera** button to start a viewer to test whether the supplied information is correct.

   **What if my camera is not is not listed in the Add Camera Wizard?**

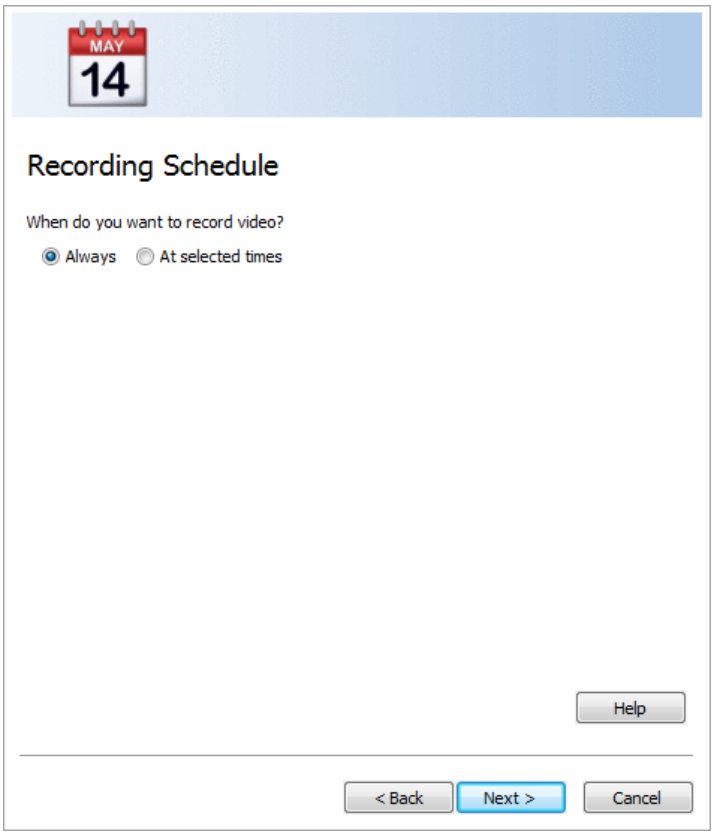
   If your camera is not listed in the Add Camera Wizard, you'll need to add the camera's information manually using the Camera Configurations window for IP cameras. See Manually Add IP Camera for this procedure.

7. Click **Next** for the Description window.



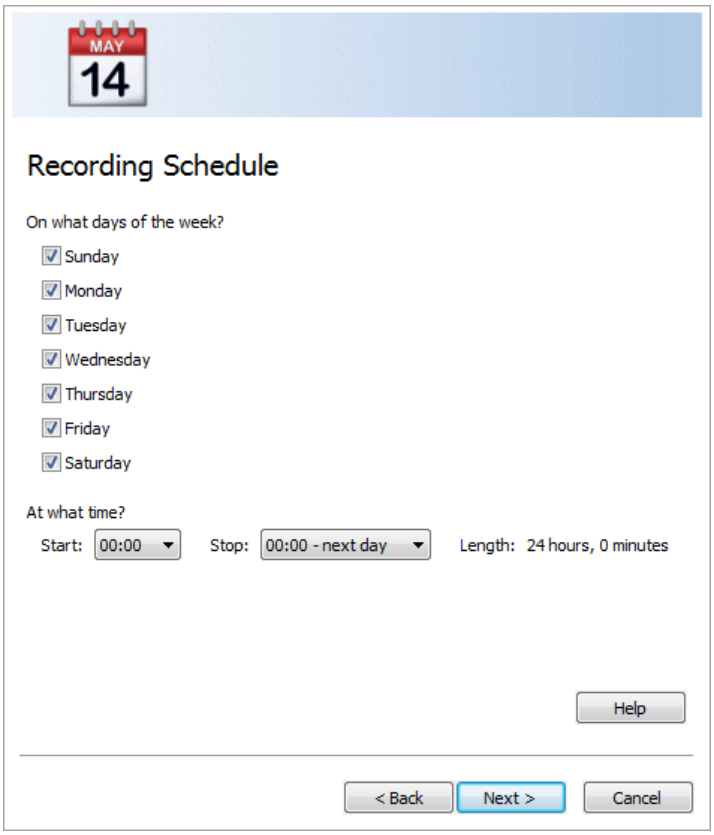

8. In the **What is the name of this camera?** text box, type a meaningful name to identify the camera.
9. In the **Enter a brief description of this camera** text box, optionally type a short note describing the camera.
10. Click **Next** for the Recording Schedule window.

© 2015




11. Indicate when you want to record video:
    - Select **Always** to record video continuously.
    - Select **At selected times** to record only on certain days or at certain times of the day.
12. If you selected the **At selected times** option, the following window appears when the **Next** button is clicked:

© 2015

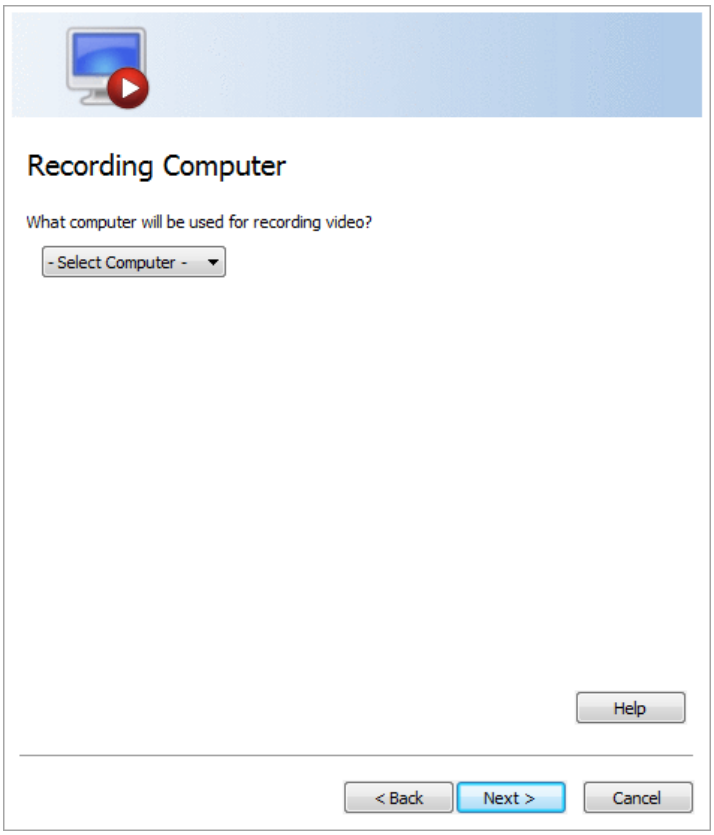



13. Use the **On what days of the week?** checkboxes to select the days to record video.

14. Use the **At what time? Start** and **Stop** drop-down lists to set the beginning and ending times for the period to record. When you make your selections, the length of the time period is indicated.

15. Click **Next** for the Recording Computer window.

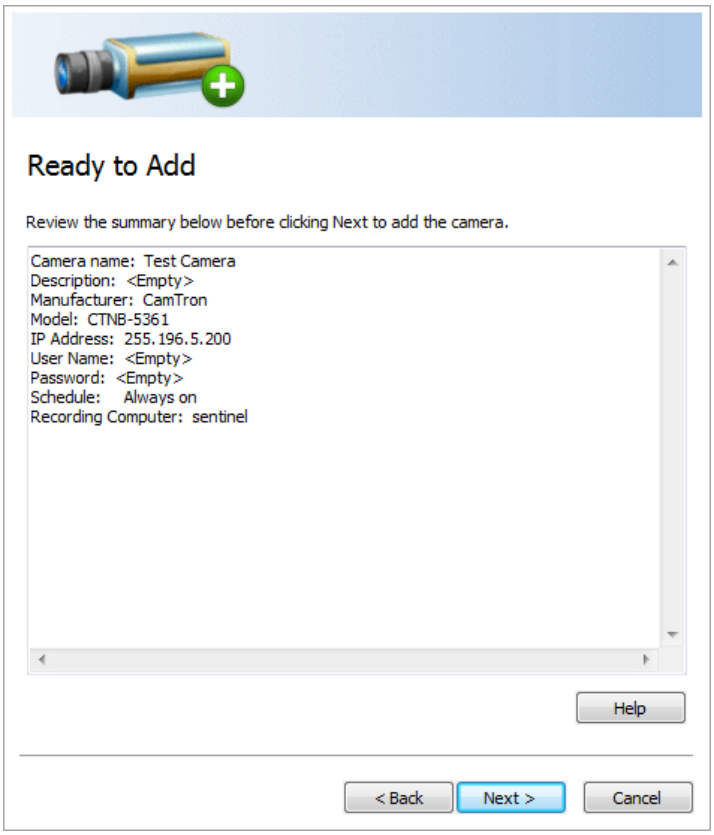
© 2015




16. From the **What computer will be used for recording video?** drop-down list, select the computer for recording video.

17. Click **Next** for the Ready to Add window.

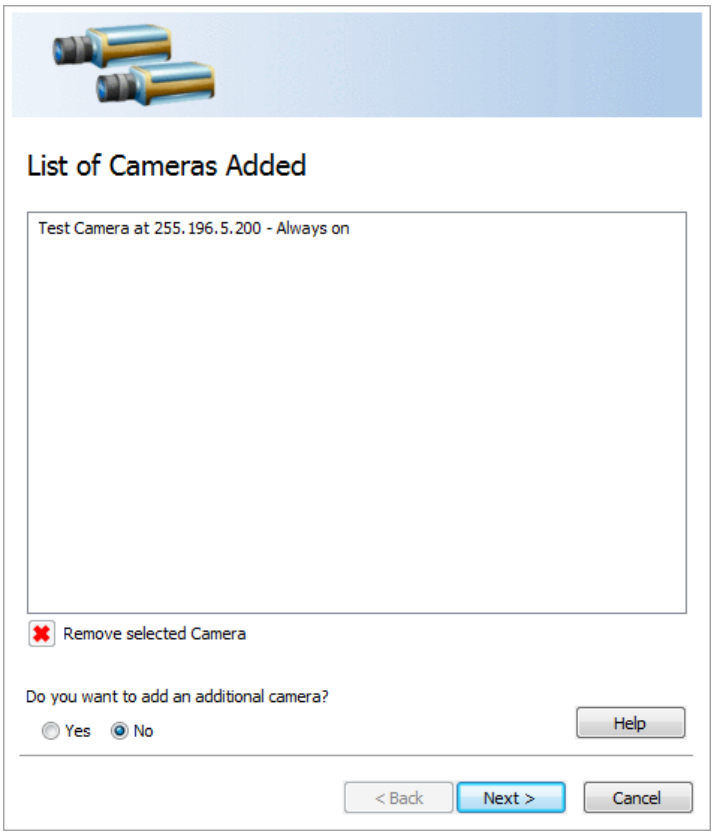
© 2015




18. Review the information. To change anything, use the **Back** button to go to the appropriate wizard screen.

19. Click **Next** for the List of Cameras Added window.

© 2015

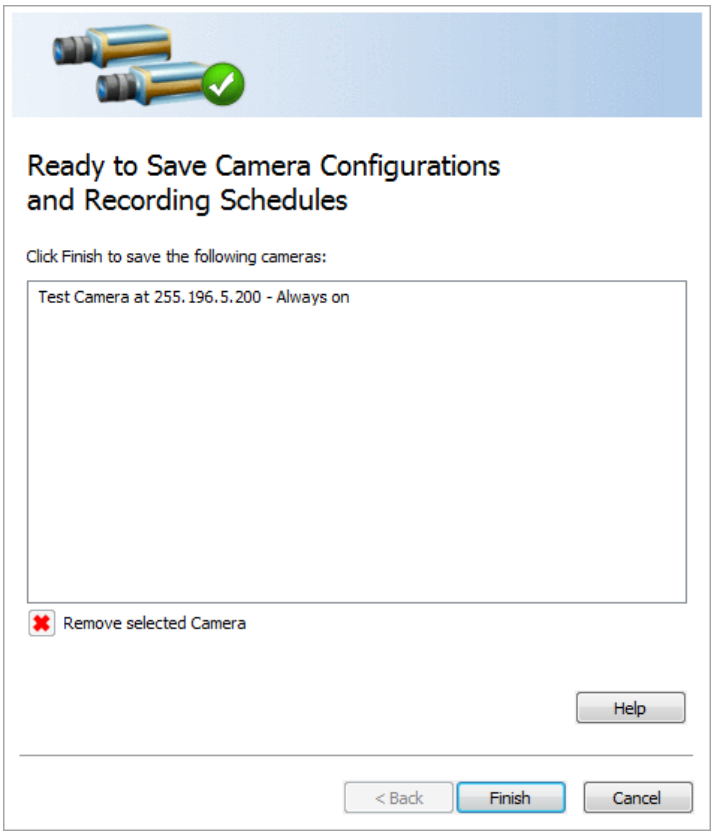



20. The cameras added during the wizard session are listed. To remove any camera, select it and then click the **Remove Selected Camera** button.

21. If you do not want to add another camera, select **No**. To add another camera, select **Yes** in order to cycle through the wizard again. Click **Next**.

22. If you have no more cameras to add, the Ready to Save Camera Configurations and Recording Schedules window appears.

© 2015




23. The list of cameras ready for saving, is displayed. To remove any camera, select it and then click the **Remove Selected Camera** button.

24. Click **Finish**. The Add Camera Wizard closes and the focus is on the main Camera Policies application window.

Through configuring a camera and setting a schedule for it to record, you created a new recording policy that is listed on the left side under the **Recording Policy Name** column of the main Camera Policies application.

## Camera Policies

Camera Policies is a critical part of your total video surveillance solution. It is responsible for getting data into the Information Repository from a camera source. The Camera Policies application generates a low resolution companion file that is a fraction of the size of the original. This preserves the original and makes it easier for fast searches and video review later in the process. Record and capture video feeds via:

- **RTSP-enabled IP cameras** - Configure RTSP-enabled IP cameras to create policies that automatically record video directly into the Information Repository.
- **VMS-managed cameras** - Configure VMS-managed cameras to create policies to capture video into the Information Repository. Depending on your hardware device and your product license, video capture from VMS may not be available.

© 2015

Camera Policies are used to control which video feeds are captured, where video is stored, when jobs start and stop, how often jobs run, and many other aspects of jobs. This information is decided by defining parameters for a camera or recording policy.

Each Camera Policy created runs independently and manages all error logging, job operation completion times, and other information for its own computer platform and file systems. Any Camera Policy can see and capture video data from any configured RTSP-enabled IP camera or VMS-managed camera.

Keep the following in mind when working with Camera Policies:

- The first time that Camera Policies is opened, the left pane is empty. Before accessing any of the tabs, create a policy.
- There can be multiple recording policies per camera, but it is not recommended to have multiple policies active and running at the same time for a single camera.
- A triangular caution symbol superimposed on a policy icon in the left pane indicates that the policy is not running. A policy does not run if its **Active** checkbox is de-selected, if the camera associated with it is not marked as active, or if there is no recording computer selected to run the policy.
- Camera Polices are visible to all computers in the Information Repository that are running Camera Polices and have appropriate permissions.
- Because recording policies are implemented across the entire Information Repository, other users can change policies while you are working in Camera Policies. To ensure that you are viewing the most current list of policies, click the **Refresh** button from the toolbar.
- Duplicate policy names are permitted.

If multiple people in your organization create or modify camera configurations or recording policies, do not attempt to make changes at the same time. Doing so may cause someone's work to be unintentionally overwritten.

## Recording Policies

The terms Camera Policy and Recording Policy may seem synonymous, but there is a slight distinction. Camera Policies encompasses all the features and functions found in the Camera Policy application. A Recording Policy refers directly to the name of the policy associated to a camera, and all the parameters to make it run. In the Camera Policies window, the left pane specifically lists all the existing recording policy names, and is saved as part of the active configuration.

Recording policies run on an assigned computer. They define when video is recorded or captured and where it goes in the Information Repository.

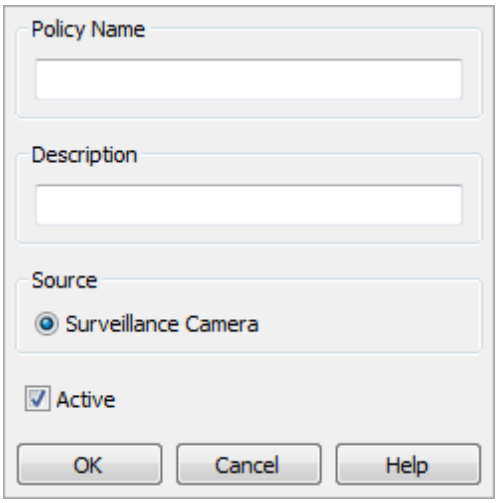
Recording policies are visible to all computers in the Information Repository that are running the Camera Policies application and that have appropriate permissions.

### Create a Policy

© 2015

The most convenient way to set up a camera, a schedule, and then record video is to use the Add Camera Wizard. However, there are times when using the wizard is not applicable, for example, if your camera information is not included in the manufacturer or model list. If using the wizard is not applicable, you must create a recording policy manually.

1. Open the Camera Policies application.
2. From the Camera Policies application toolbar, click the **Add** button to create a new policy. Or from the **Edit** menu, select **Create a Policy**.



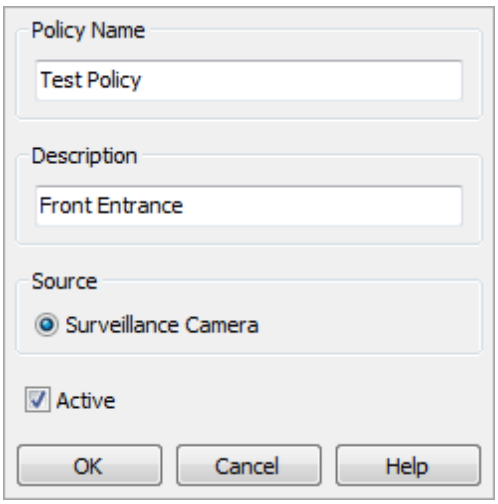

3. In the Create a Policy window, type a **Policy Name** for the new policy.
4. Type a **Description** for the new policy for quick reference.
5. The **Source** is always Surveillance Camera.
6. Select the policy as active, or de-select the **Active** checkbox if you do not want the policy to run. When the **Active** checkbox is de-selected, the triangular caution symbol is superimposed over the policy in the Camera Policies window left pane - **Recording Policy Name** column.
7. Click **OK**. The window closes, and the Recording Policy Name, Camera, Recording Computer, and Description appear in the Camera Policies.
8. On the **Camera** tab, from the **Camera** drop-down list, select the camera configuration that the policy applies to.
9. (Advanced mode only) On the **Processing** tab, define video and file processing options.
10. (Advanced mode only) On the **Destination** tab, define the Vault, media, storage pool, and other options where video is recorded or captured to.
11. On the **Scheduling** tab, select when to record video.
12. (Advanced mode only) On the **Advanced** tab, select log and report, or performance options.
13. Click the **Save** button to save all policy settings and implement the policy.

© 2015

Open Network Activity to monitor processing as policies are created.

## Modify a Policy

1. From the Camera Policies left pane, double click an existing policy name. Or, from the **Edit** menu, select **Modify Selected Policy**. The Modify Selected Policy window opens for the selected policy.




2. Type a new policy name or a new description.
3. Select the policy as active, or de-select the **Active** checkbox if you do not want the policy to run. When the **Active** checkbox is de-selected, the triangular caution symbol is superimposed over the policy in the Camera Policies window left pane - **Recording Policy Name** column.
4. Click **OK**. The window closes, and the Recording Policy Name, Camera, Recording Computer, and Description appear in the Camera Policies.
5. Modify policy parameters as needed for each Camera Policies tab.
6. Click the **Save** button to save all policy settings and implement the policy.

If another user on the network makes changes to a policy while you have the Camera Policies application open, there will be a popup message asking if you would like to refresh your view in order to see the most recent changes. Clicking **Yes** to refresh your view will cause you to lose any of your unsaved work or changes. Click **No** to continue modifying a policy without refreshing your view. This may cause you to accidentally overwrite the changes the other user made.

© 2015

If you modify a recording policy while a job is running that is based on that policy, the job stops as soon as it is finished processing the current file. The job restarts as scheduled. For example, a job runs every day at 11:00 AM for 30 minutes. While the job is running, the policy is modified and the job stops. If the scheduled start time was not changed, the job starts at 11:00 AM the next day.

### Delete a Policy

You can delete a policy that no longer meets your needs, or you can de-activate a policy and then re-activate it at a later time if needed.

**To delete a policy:**

1. From the Camera Policies window left pane - **Recording Policy Name** column, click the policy to delete.
2. Click the **Delete** button .
3. After deletion of a policy, Camera Policies has been modified. Click the **Save** button to save the updated Camera Policy settings.

If you delete a policy while a job is running, the job stops as soon as it is finished processing the current file.

**To make an active policy inactive:**

1. From the Camera Policies window left pane - **Recording Policy Name** column, double-click the policy.
2. In the **Modify Selected Policy** window, de-select the **Active** checkbox.

## Import/Export Recording Policies

Policy import and export functionality offered by SoleraTec's Phoenix RSM allows you to save policies, restore policies, and copy sets of policies from one computer to another. After creating a set of policies, you can export them to a policy file. Then, at a later time, if you want to re-implement the set of policies or implement them for the first time on another computer, they are there for import.

Use the import and export functionality to take a snapshot of the working policy configuration, bring new computers online, test different policy configurations, or restore user corrupted policy configurations.

By default, recording policies are exported to **CameraPolicies.cfg**. Data service policies are exported to **DataSvcsSvc.cfg**.

Although each policy editor uses only one policy set at a time, multiple policy sets exported to policy files can be used. Create, name, and use any file naming convention for policy files. Be sure to keep track of where policies are exported to if it is a location other than the default location (the user's home directory).

© 2015

Before restoring a set of policies to a computer that currently has policies set up, be sure to delete all of the current policies - otherwise imported policies are added to current policies.

Camera policies are incompatible with other client policies and vice versa. If you try to import a Camera policy into a non-Camera policies client (or vice versa), an error message appears and no policies are added.

## Import Policies

When importing policies, they are added to the policies that are already in the policy editor.

1. From the application's main menu (or policy editor), click **File** > **Import from**. The Import from window appears.
2. If you are not importing policies from your local computer, navigate to the networked computer that contains the policies that you need.
3. Select the policy file that contains the policies that you want to use.
4. Click **Open**. The policies in the configuration file are implemented.

## Export Policies

1. Create policies.
2. From the application's main menu (or policy editor), click **File** > **Export to**. The Export to window appears.
3. To save your policies with the default policy file name, click **Save** without entering a new file name. Or, enter a new name in the File name text box, and then click **Save**.

## Import/Export Policy File Structure

An exported policy file is block structured but free from any column or order formatting. The tokens listed below specify job criteria. By default, policy files are exported to and imported from the locations below:

| | |
|---|---|
| Camera Policies | <install-dir>/Config/CameraPolicies.cfg. |

Files that contain policies are formatted as follows. Each policy is a single block. The beginning of each block is indicated by policy_name="<policy name>".

```
policy_name="<policy name>"
[
    <token>=<value>
    <token>=<value>
    . . .
]
```

© 2015

```
policy_name="<policy name>"
[
    <token>=<value>
    <token>=<value>
    . . .
]
. . .
```

## Token/Value Pairs

A token is a job attribute that is given a value to determine how a job runs.

Depending on your current software version, some of the Token/Value pairs may not apply.

| Token/Value | Description |
|---|---|
| act_log_enabled = <*boolean*> | Enable the creation of activity logs.<br>Valid values: true \| false<br>Default = false |
| act_log_pn = "<*pathname*>" | Define the path for the activity log. Supports token substitution.<br>Default path = "%R/Logs/%P.act" |
| absolute_start = <*yyyy*>/<*mm*><br>/<*dd*>-<*hh*>:<*mm*>:<*ss*> | The exact start time and date that the job is to run. Multiple absolute start tokens may be entered.[1, 2] |
| active = <*boolean*> | Define if the policy is active or inactive.[2]<br>Valid values = true \| false<br>Default = true |
| admin_pn = "<*pathname*>" | The directory that contains the log, retry, and history files. Supports token substitution.<br>Default path = "<install-dir>/JobHistory/" |
| any_user_retrieve = <*boolean*> | Allows any user to retrieve a file in the job, regardless of the initial read access.<br>Valid values = true \| false<br>Default = false |
| backup_data | Internal use only. |
| backup_stub | Internal use only. |

© 2015

| | |
|---|---|
| complete = <*boolean*> | Print all summary information plus the path names of the files ingested to the file indicated by the list_pn option.<br>Valid values = true \| false<br>Default = false |
| compress | Internal use only. |
| create_job_history = <*boolean*> | Create job history files for each job.<br>Valid values = true \| false<br>Default = false |
| data_paths = <*number*> | The maximum number of concurrent files that can be sent.<br>Default = 1 |
| description = "<*character string*>" | A description of the policy.[2]<br>Default = blank |
| diag = <*boolean*> | Print diagnostic information to the file indicated by the list_pn option.<br>Valid values = true \| false<br>Default = false |
| dir_spec = "<*pathname*>" | Directories to include. Multiple dir_spec options can be specified. The dir_spec check is made for every directory found. This includes the directories contained in the path name list that the job traverses.<br>Default = "*" (any) |
| display_only = <*boolean*> | Cause job to search for but not store targeted files. List the files that would have been ingested.<br>Valid values = true \| false<br>Default = false |
| dst_local_only = <*boolean*> | Cause job to use only a Vault local to the computer from where service is running.<br>Valid values = true \| false<br>Default = false |

© 2015

| | |
|---|---|
| dst_media_name = "<*character string*>" | The destination media to be used. If not specified, the first available unit of media is used.<br><br>Default = "*" (any) |
| dst_media_speed = "<*character string*>" | The destination media to be used according to media speed.<br><br>Valid values =<br>• S0 - S10<br>• Unspecified<br><br>Default = Unspecified |
| dst_media_type = "<*character string*>" | The media type to be used for a job.<br><br>Valid values =<br>• Hdisk – Hard disk<br>• 8mm – Eight-millimeter tape<br>• Dds – Digital data storage<br>• Dlt – Digital linear tape<br>• Ait – Advanced intelligent tape<br>• SuperAit<br>• Vxa - Exabyte Vxa tape<br>• Travan - Travan tape<br>• Lto – Linear tape open<br>• MagOptical – Read/write optical<br>• NullDevice<br>• Unspecified<br><br>Default = Unspecified |
| dst_storage_pool = "<*alpha*>" | The name of the destination storage pool. Use "" for no storage pool name.<br><br>Default = "*" (any) |
| dst_vault_name = "<*character string*>" | The destination Vault name. If not specified, the first available Vault is used.<br><br>Default = "*" (any) |

© 2015

| | |
|---|---|
| dst_volume_format | Internal use only. |
| dst_volume_name | Internal use only. |
| dst_volume_pack | Internal use only. |
| dtu_type = <*alpha*><*yyyy*>/<*mm*> /<*dd*>-<*hh*>:<*mm*>:<*ss*><br><br>or<br><br>dtu_type = L<*level*> | Ingest files based on time and date or job level.<br><br>Valid values =<br><br>• AO (Absolute Old) – Select files with a dtu (date_time_use) equal to or before the specified date. Enter the year as a 4-digit number.<br>• AN (Absolute New) – Select files with a dtu equal to or after the specified date. Enter the year as a 4-digit number.<br>• RO (Relative Old) – Select files with a dtu equal to or before the relative specified date.<br>• RN (Relative New) – Select files with a dtu equal to or after the relative specified date.<br>• L0 – Ingest all files.<br>• L1 – Ingest all data changed since the last L0 job.<br>• L2 – Ingest all data changed since the last L1 job.<br>• L3 – Ingest all data changed since the last L2 job.<br>• L4 – Ingest all data changed since the last L3 job.<br><br>Default = L0 |
| error_log = "<*pathname*>" | The path for the error log file. If you specify "/dev/tty", error messages display on the default output device. Supports token substitution.<br><br>Default path for the configuration file = "R/Logs/%P.err" |
| exclude_dir_spec = "<*pathname*>" | Omit directories. Accept multiple instances. |

© 2015

| | |
|---|---|
| | Default = "" (no directories excluded) |
| exclude_file_spec = "<*pathname*>" | Omit files. Accept multiple instances.<br><br>Default = "" (no files excluded) |
| ext_metadata = "<*command*>" | Extended metadata in a token/value pairs. Token/values can be found in the MetadataExtensions.cfg section..<br><br>Format:<br><br>token="<command>"token="<command>"...<br><br>Default = "" |
| ext_metadata_plugin = "<*character string*>" | Enable the collection of extended metadata.<br><br>Default = "EmdProcessNone" |
| file_grouping_plugin = "<*character string*>" | Enable file grouping.<br><br>Default = "FgProcessNone" |
| file_spec = "< *pathname*>" | Files to be ingested. This token/value pair can be specified multiple times to include multiple file filters.<br><br>Default = "*" (any) |
| follow_links | Internal use only. |
| host_Id = "<*character string*>" | Where the Target and Process Service runs.[2]<br><br>Default = blank |
| include_offline | Internal use only. |
| job_type = <*alpha*> | Specify the job type.<br><br>Valid values =<br><br>• backup<br>• move<br><br>Default = backup |
| list_pn = "<*pathname*>" | The filename where all report information is written. Supports token substitution.<br><br>Default path for the configuration file is "%R/Logs/%P.log" |

© 2015

| | |
|---|---|
| local_only = <*boolean*> | Specify that the ingested file is to reside on the local computer.<br>Valid values = true \| false<br>Default = true |
| localize = <*boolean*> | All subsequent files in the same job are sent to the same unit of media until it is full.<br>Valid values = true \| false<br>Default = true |
| lock_vault | Internal use only. |
| obj_type = "<*character string*>" | The policy source.<br>Valid values =<br>• native_fs<br>• mse_pst<br>• mse_msg<br>• surv_camera<br>Default = native_fs |
| out_of_band = <*boolean*> | Enable the application to constantly monitor its processes and select the network transmission protocol that best suits the files being processed.<br>Valid values = true \| false<br>Default = true |
| pathname = "<*pathname*>" | The path name that is searched for files matching the options. Files, directories, and wildcard expressions are valid. This token/value pair can be specified multiple times to include multiple paths.<br>No default |
| pict_gen_preview_image = <*boolean*> | Generate preview image thumbnails at capture/ingest.<br>Valid values = true \| false<br>Default = true |

© 2015

| | |
|---|---|
| pict_preview_image_quality = <*boolean*> | Determine the quality of the preview image.<br>Valid values = High \| Medium \| Low<br>Default = Medium |
| pict_process_components = <*boolean*> | Capture/ingest picture files so that they are readable by search applications.<br>Valid values = true \| false<br>Default = false |
| pict_save_preview_image = <*boolean*> | Save a preview image at the path entered in pict_save_preview_image_dir_pn.<br>Valid values = true \| false<br>Default = false |
| pict_save_preview_image_dir_pn = "<*pathname*>" | The path where the copy of the preview image is saved.<br>Default path = "" |
| policy_name = "<*policy name*>" | The job identifier.<br>No default |
| post_proc_cmd = "<*command*>" | A post-process command that runs immediately after the job is finished. Supports token substitution.<br>Default = "" |
| pre_proc_cmd = "<*command*>" | A pre-process command that runs immediately before the job starts. Supports token substitution.<br>Default = "" |
| process_directories = <*boolean*> | Preserve the state of directories.<br>Valid values = true \| false<br>Default = true |
| ref_id = "<*character string*>" | Internal use only. |
| repeat_interval = <*hh:mm:ss*> | The amount of time that elapses before a job is repeated.[1, 2]<br>Default = 24:00:00 |

© 2015

| | |
|---|---|
| retry_time = <*alpha*><*yyyy*>/<*mm*>/<*dd*>-<*hh*>:<*mm*>:<*ss*> | The date and time to retry the list of files not ingested. These files match all job criteria but were not sent to the Vault. You must precede the date/time value with an **A** to specify an absolute date and time or an **R** to specify a date and time relative to the end of the job. Enter the absolute year as a four-digit number (for example, 2001, 2002, etc.).<br>Valid values =<br>• A – Absolute date and time.<br>• R – Relative date and time.<br>Default = R0000/00/00-00:00:00 (retry files immediately after the job finishes) |
| start_days = <*mtwtfss*> | The days the job runs. Use **-** to indicate days the job should not run.<br>For example, if the job is to run on Thursday, you would enter ---t---.[1, 2]<br>Default = mtwtfss |
| start_time = <*hh:mm:ss*> | The time the job should start for each defined start day in start_days.[1, 2]<br>Default = 00:00:00 (midnight) |
| stop_time = R<*yyyy*>/<*mm*>/<*dd*>-<*hh*>:<*mm*>:<ss> | The date and time the job is to stop. The date and time entered is relative to the start of the job.<br>R = relative to the start of the job.<br>Default = R0000/00/00-00:00:00 (no stop time) |
| summary = <*boolean*> | Print the start and finish times of the job and the final statistics to the file indicated by the list_pn option.<br>Valid values = true \| false<br>Default = true |
| system_info = <*boolean*> | Ingest system info and other system states.<br>Valid values = true \| false<br>Default = false |

© 2015

| | |
|---|---|
| throttle = <*setting*> | The throttle controls the amount of bandwidth used by jobs (and, the speed files are sent to Vaults). Throttle values are relative to Information Repository capacity and range from 1% to 100%. A lower setting reduces the amount of available bandwidth that is used.<br>Default = 100 |
| timestamp = <*alpha*> | Specify the timestamp of the file that is to be examined when determining if the file meets the dtu_type criteria.<br>• atime - access time<br>• mtime - modified time<br>Default = mtime |
| type = <*alpha*> | The policy type of the policy file.[2]<br>Default = tap |
| update_run_record = <*boolean*> | Update the job run record (<install-dir>/ JobHistory/run_record.trr) whenever a "level" job runs.<br>Valid values = true \| false<br>Default = true |
| vcs = <*alpha*><*max num files*> | The number of files (F) or number of bytes (S) to ingest per single Vault connection.<br>Valid values =<br>• F – files<br>• S – bytes<br>• 1 - ∞<br>Default = F500 |
| version = <*number*> | The version number of the policy. The current version is 1.0.[2] |
| vid_extract_closed_caption = <*boolean*> | Extract closed captioning data from a video at ingest.<br>Valid values = true \| false<br>Default = true |

© 2015

| | |
|---|---|
| vid_gen_low_res_proxy = <*boolean*> | Generate low resolution proxy videos at capture/ingest.<br>Valid values = true \| false<br>Default = true |
| vid_gen_preview_image = <*boolean*> | Generate preview image thumbnails at capture/ingest.<br>Valid values = true \| false<br>Default = true |
| vid_low_res_proxy_fr_denom = <*integer*> | The frame rate at which the LRP will be generated.<br>Default = 1 |
| vid_low_res_proxy_quality = <*setting*> | Determine the quality of the low resolution proxy video.<br>Valid values = High \| Medium \| Low<br>Default = Medium |
| vid_preview_image_quality = <*setting*> | Determine the quality of the preview image.<br>Valid values = High \| Medium \| Low<br>Default = Medium |
| vid_process_components = <*boolean*> | Capture/ingest video files so they are readable by Phoenix RSM search applications.<br>Valid values = true \| false<br>Default = false |
| vid_save_closed_caption = <*boolean*> | Save a copy of the closed captioning data in a location specified by vid_save_closed_caption_dir_pn.<br>Valid values = true \| false<br>Default = false |
| vid_save_closed_caption_dir_pn = "<*pathname*>" | The path where the closed captioning file is saved.<br>Default path = "" |

© 2015

| | |
|---|---|
| vid_save_low_res_proxy = <*boolean*> | Save a copy of the low resolution proxy video at the location entered in vid_save_low_res_proxy_dir_pn.<br>Valid values = true \| false<br>Default = false |
| vid_save_low_res_proxy_dir_pn = "<*pathname*>" | The path where the copy of the low resolution proxy video is saved.<br>Default path = "" |
| vid_save_preview_image = <*boolean*> | Save a preview image at the path entered in vid_save_preview_image_dir_pn.<br>Valid values = true \| false<br>Default = false |
| vid_save_preview_image_dir_pn = "<*pathname*>" | The path where the copy of the preview image is saved.<br>Default path = "" |

[1]**Note:** Timing tokens are mutually exclusive. Only one timing token may be set. In other words, you may set either absolute_start, or repeat_interval, or start_days and start_time.

[2]**Note:** Token/Value pair is used for policy only.

### Camera

| Token/Value | Description |
|---|---|
| camera_cache_pn = "<*character string*>" | The location of the cache to hold the clips before sending to Vault.<br>Default is “” |
| camera_clip_duration = <*integer*> | The length of clip that incoming video streams are captured into.<br>Default = 300 seconds |
| camera_motion_detect = <*boolean*> | Determine if motion detection data is captured from RTSP enabled IP cameras that support motion detection. If selected for cameras that do not capture motion detection data or otherwise are not supported, no motion detection data is preserved. |

© 2015

| Token/Value | Description |
|---|---|
| | Default = true |
| camera_name = "<*character string*> " | The name of the camera.<br>Default = "" |
| camera_use_config = <*boolean*> | Use the camera information found in the Camera Configurations for the selected camera.<br>Default = true |

## Sample Recording Policy

If you were to export a policy, it would look similar to the following:

```
#
# Start of object rule for policy_name 'Rear_Deck'
#
policy_name = "Rear_Deck"
[
    type                                = "tap"
    version                             = "1.0"
    active                              = true
    job_type                            = move
    obj_type                            = "surv_camera"
    description                         = "Record video from 'Rear Deck'"
    dtu_type                            = L0
    local_only                          = false
    follow_links                        = false
    process_directories                 = false
    timestamp                           = mtime
    backup_stub                         = false
    backup_data                         = false
    include_offline                     = false
    dst_media_type                      = Unspecified
    dst_media_speed                     = Unspecified
    dst_volume_format                   = Unspecified
    dst_vault_name                      = "*"
    dst_media_name                      = "*"
    dst_volume_name                     = "*"
    dst_storage_pool                    = "*"
    dst_volume_pack                     = ""
    dst_local_only                      = true
    localize                            = false
    repeat_interval                     = 00:00:05
    stop_time                           = R0000/00/00-00:00:00
    pre_proc_cmd                        = ""
```

```
    post_proc_cmd                       = ""
    error_log                           = "%R/Logs/%P.err"
    summary                             = true
    complete                            = false
    diag                                = false
    list_pn                             = "%R/Logs/%P.log"
    display_only                        = false
    update_run_record                   = false
    create_job_history                  = false
    retry_time                          = R0000/00/00-00:00:00
    any_user_retrieve                   = true
    out_of_band                         = true
    vcs                                 = F1
    data_paths                          = 1
    throttle                            = 100
    system_info                         = false
    act_log_enabled                     = false
    act_log_pn                          = "%R/Logs/%P.act"
    ext_metadata_plugin                 = "EmdProcessNone"
    file_grouping_plugin                = "FgProcessNone"
    vid_process_components              = true
    vid_gen_low_res_proxy               = true
    vid_low_res_proxy_quality           = Medium
    vid_save_low_res_proxy              = false
    vid_save_low_res_proxy_dir_pn       = ""
    vid_gen_preview_image               = true
    vid_preview_image_quality           = Low
    vid_save_preview_image              = false
    vid_save_preview_image_dir_pn       = ""
    vid_extract_closed_caption          = false
    vid_save_closed_caption             = false
    vid_save_closed_caption_dir_pn      = ""
    pict_process_components             = false
    pict_gen_preview_image              = true
    pict_preview_image_quality          = Medium
    pict_save_preview_image             = false
    pict_save_preview_image_dir_pn      = ""
    ext_metadata                        = ""
    camera_name                         = "Camera 210 Rear View"
    camera_use_config                   = true
    camera_clip_duration                = 300
    camera_cache_pn                     = ""
    camera_motion_detect                = true
    ref_id                              = 4b2797282db811e1a154000c29100a64
    compress                            = false
    lock_vault                          = true
]
# end of object rule for policy_name 'Rear_Deck'
```

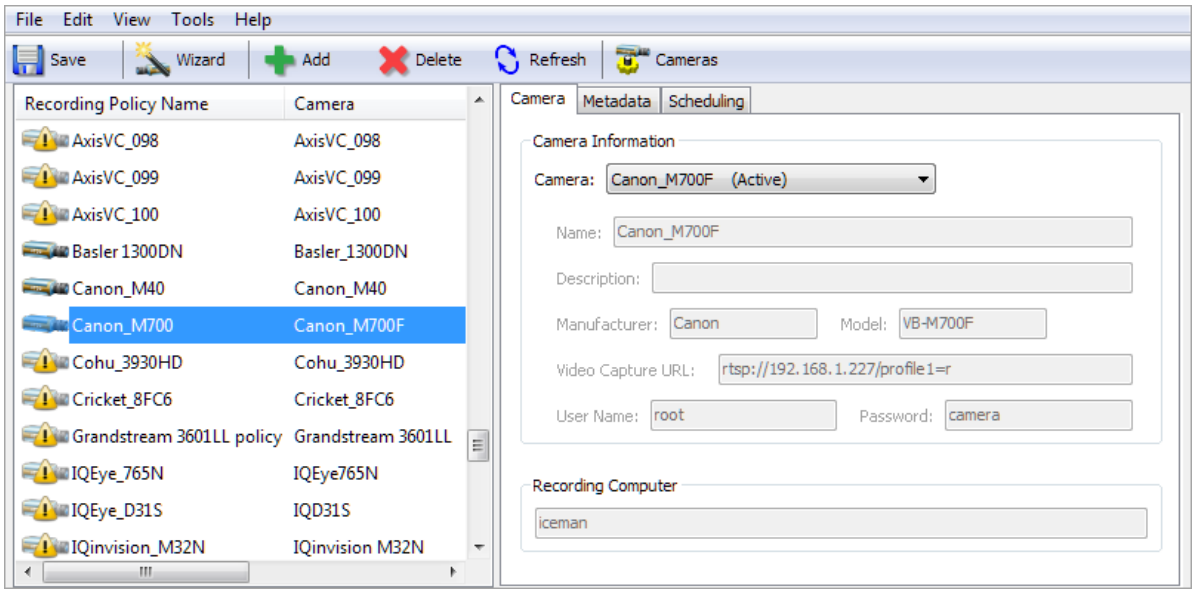
# Camera Policies Window

The main Camera Policies window is divided into two main panes: the right pane contains the tabs you will need to populate in order to create a policy and the left pane provides an overview of all of the recording policies in the Information Repository. Overview information includes the Recording Policy Name, Camera, Recording Computer, and a Policy Description. When you move your mouse over a policy listed in the left pane, a small popup displays summary information about the Recording Policy.

There are also two modes that Camera Policies can run in: **Standard** mode and **Advanced** mode. After initial install of the Camera Policies application, the default setting opens in **Standard** mode. The **Advanced** mode reveals more features and options available to Camera Policies.

The Camera Policies toolbar consists of the following buttons:

- Save all policy settings.
- Open the Add Camera Wizard to easily configure a camera and schedule it to record video automatically.
- Add a new policy.
- Delete the selected policy.
- Refresh the Camera Policies view to see the latest version of each policy displayed.
- Open the Camera Configurations window.

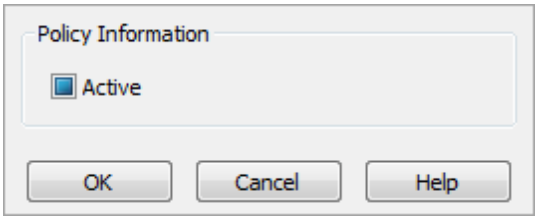



A triangular caution symbol on the policy icon in the left pane of the window indicates that the policy is not active.

© 2015

From the left pane, you can edit the **Active** setting of a policy. Setting a policy to **Active** allows the policy to run. You can edit the active setting of policies by right-clicking on an individual policy or multiple selected policies (select multiple policies by holding the**Shift** key or the **Control** key and clicking on the desired policies), choosing **Change Active Setting** from the shortcut menu, either selecting or de-selecting the **Active** option in the dialog box, and then clicking **OK**. Click the **Save** button in the toolbar to implement any changes immediately.

When multiple policies are selected with different current active settings, the checkbox will be shaded to indicate the selected policies have different **Active Settings**.




## Camera Policies Menu Items

| Menu Items | Description |
|---|---|
| **File > Save All** | Save the information for all the current policies. |
| **File > Import from** | Open an Import from dialog box to navigate to and select a camera configurations file. |
| **File > Export to** | Open an Export to dialog box to navigate to and select where to save the active camera configurations file. |
| **File > Exit** | Close the application. If changes have been made a Confirmation dialog box appears for saving changes, click **Yes**, **No**, or **Cancel**. |
| **Edit > Create a Policy** | Open Create a Policy window. |
| **Edit > Modify Selected Policy** | Select a policy listed in the left pane, then select this menu item to modify the existing policy. |
| **Edit > Delete Selected Policy** | Select a policy listed in the left pane, then select this menu item to remove the policy from Camera Policies. |
| **Edit > Delete All Policies** | Delete all the policies from the configuration file, and removes policies listed in the left pane. |
| **View > Refresh Policy View** | Refresh the view in the left pane for the latest list of policies. |

© 2015

| Menu Items | Description |
|---|---|
| **View > Enable Tool Tips** | Check mark by this menu item indicates that tool tips for the window display. The tips are brief descriptions of window controls if the mouse pointer is moved over a control. De-select to turn tool tips off. |
| **View > Enable Policy Tips** | Check mark by this menu item indicates that policy tips display in the left pane. Policy tips provide details of the recording policy. De-select to turn policy tips off. |
| **View > Enable Advanced Mode** | Check mark by this menu item sets the Camera Policies window to unlock **Advanced** mode features and options. See Advanced Mode for more information. |
| **Tools > User Preferences** | **Advanced mode only.**<br><br>Open the Camera Policies User Preferences window.<br><br>User Preferences define default settings for the Camera Policies window. The information in User Preferences is the exact same as what is displayed on the **Processing** tab. User preferences are a convenient way to set your commonly used options for the desktop client running Camera Policies, and each subsequent time you run a job using your desktop client those settings are automatically set. You can make changes using the **Processing** tab, but those changes do not save as User Preferences and options reset to defaults for subsequent uses. |
| **Tools > Cameras** | Open the Camera Configurations window. Use to manually add and configure cameras to your Information Repository. You must use the Camera Configurations when capturing video from a VMS. The policy you create enables video to be retrieved from the VMS. |
| **Tools > Find Cameras** | **Advanced mode only.**<br><br>Select **Find Cameras** to open the Search Results window which shows a list of cameras found on the network.<br><br>If your camera is not on the list, select the **Show all devices** checkbox for any additional cameras on the network and other devices to display. Cameras in use appear grayed-out and available cameras for configuration have an asterisk (*) in the first column. Select a camera and click **OK**, or double-click the camera item for the camera information to configure. |

© 2015

| Menu Items | Description |
|---|---|
| **Tools > Add Camera Wizard** | Open the Add Camera Wizard to introduce and add a RTSP-enabled IP camera directly to your video surveillance solution. When you use the wizard, the process is simple and quick. A camera policy automatically gets created for the new camera.<br><br>Do not use the wizard if adding a VMS-managed camera; use Camera Configurations instead. |
| **Help > Current Page** | Open online help to the Camera Policies webpage. |
| **Help > Camera Policies Overview** | Open online help with focus on Camera Policies. |
| **Help > Contents** | Open the local version of online help. |
| **Help > Online Help** | Open the web-based version of online help. |
| **Help > Online Support** | Open the support webpage. |
| **Help > About Camera Policies** | Open the About Camera Policies window. |

## Camera Policies Advanced Mode

The default **Standard** mode setting allows you to create a recording policy by connecting and configuring RTSP-enabled IP cameras and scheduling jobs using the **Camera** and **Scheduling** tabs of the Camera Policies application.

Change the mode to the advanced setting to capture video from a video management system (VMS) such as Milestone, OnSSI, or exacqVision. Also, use the **Advanced** mode to access additional, more refined options for direct-connect IP cameras.

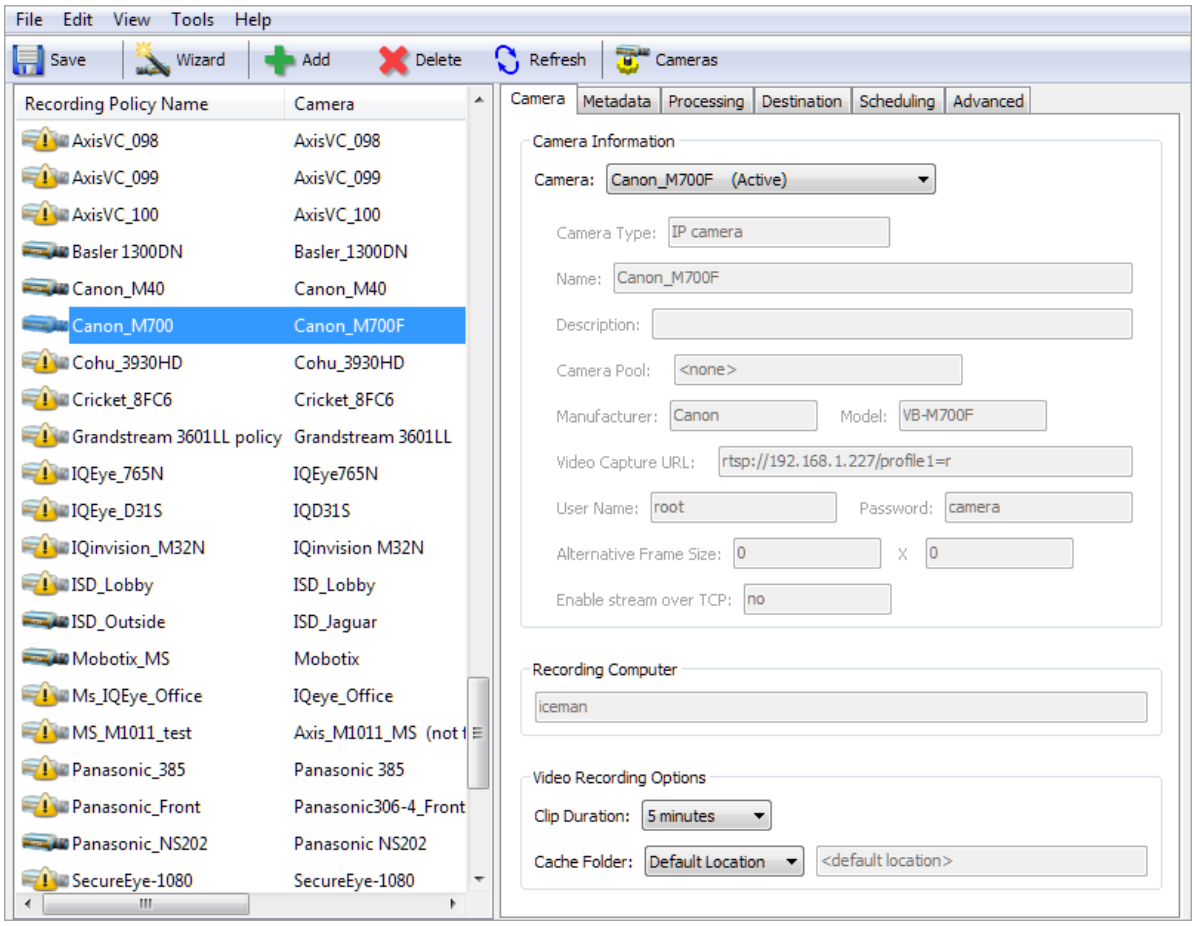
Compared to **Standard** mode, **Advanced** mode displays more features on the Camera Policies **Camera** tab and Camera Configuration window. Plus, additional tabs appear in Camera Policies: **Processing**, **Destination**, and **Advanced**. (**Standard** mode just displays **Camera** and **Scheduling** tabs.)

To make additional tabs and options available, select from the **View** menu > **Enable Advanced mode** for **Advanced** mode. If you turn **Advanced** mode on, it remains that way until you disable it.

If you set an advanced option and later want to change it, you must be in **Advanced** mode in order to access the option. Keep in mind that some Phoenix RSM users on your network may be using **Standard** mode and might not see a change in an advanced setting.

The **Advanced** mode descriptions are included in the above Camera Policies Menu Items section.

© 2015




## Camera Policies Camera Tab

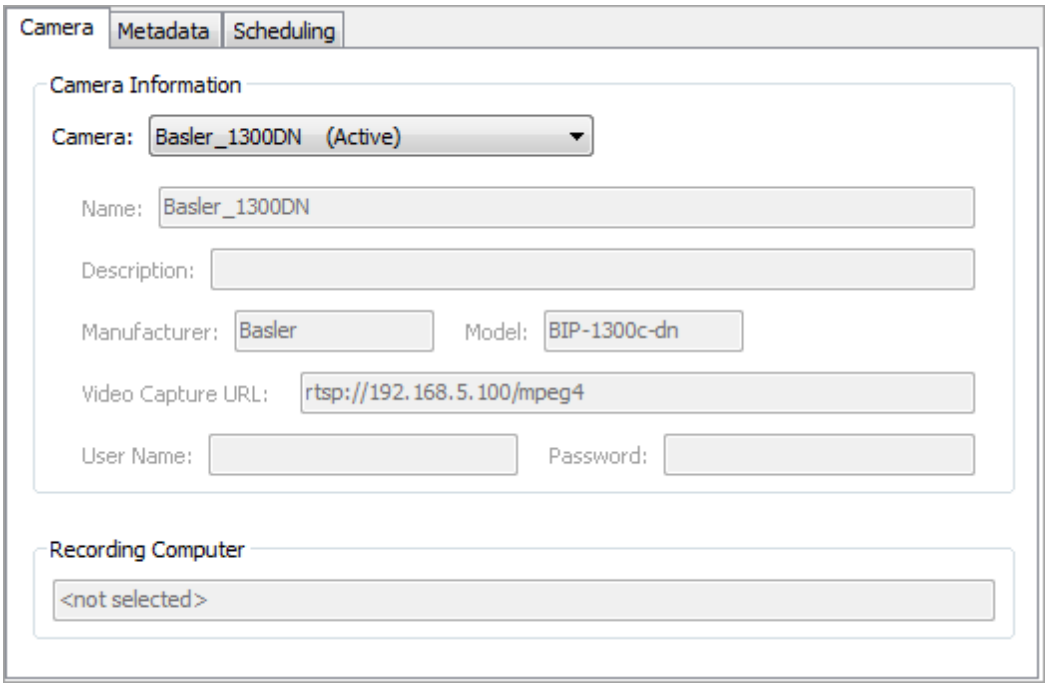
After you have connected to a camera for your video surveillance solution, create a recording policy through either the Add Camera Wizard or manually through Camera Policies Camera Configuration.

The Camera Policies **Camera** tab displays camera and recording information. If you have used the Add Camera Wizard, the information from the wizard is populated into the **Camera** tab fields. If you have built a new recording policy manually, then the information is populated from Camera Configurations, leaving only a few fields editable. Once the recording policy is created, if you select it from the Camera Policies left pane, its associated information populates the tabs.

To be able to view and record live video feeds, make sure that RTSP is enabled on your IP camera. See your camera's documentation for details on enabling RTSP.

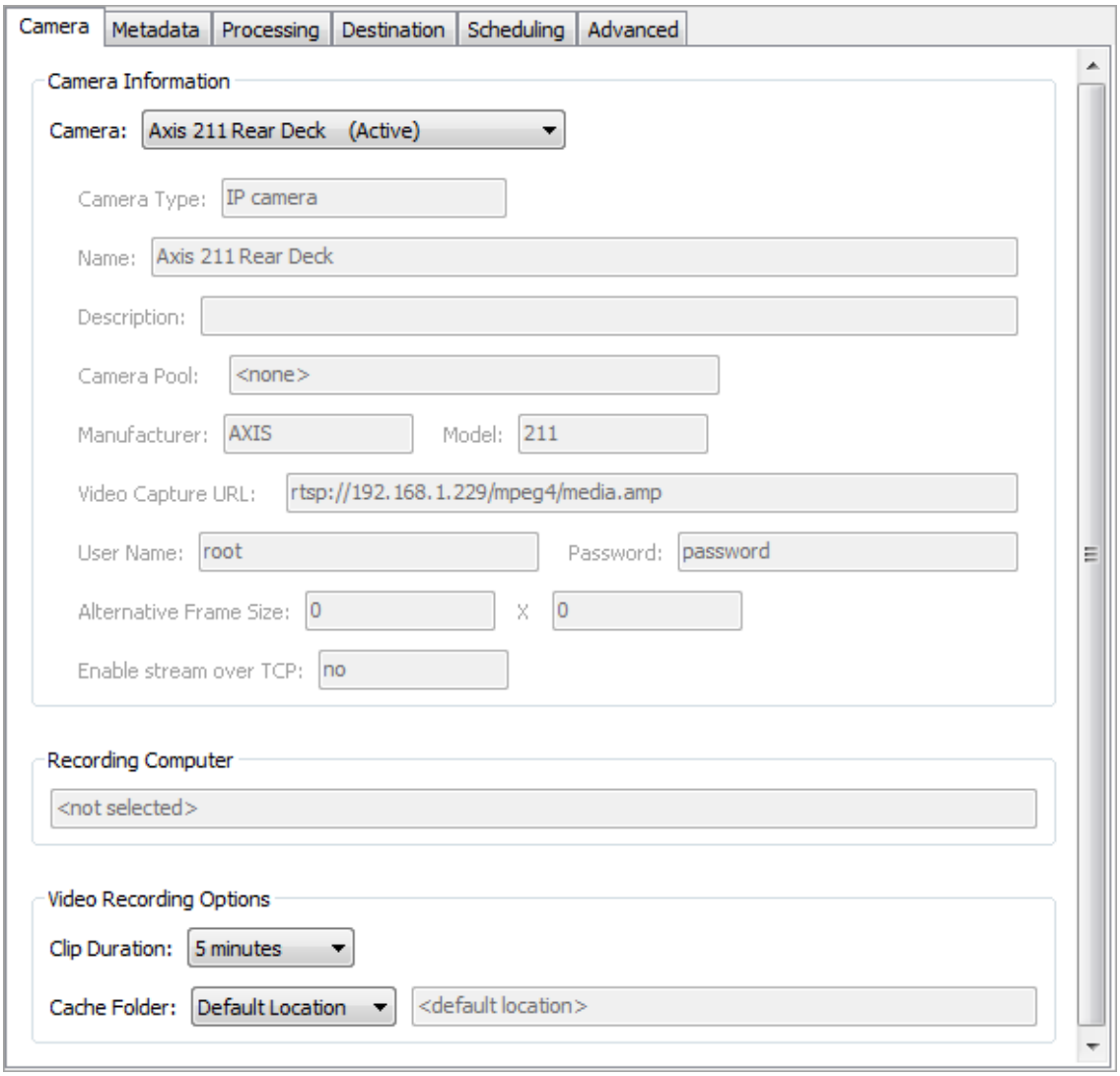
The **Camera** tab displays differently depending on whether you are working in **Standard** mode or **Advanced** mode. When **Advanced** mode is enabled, more options are available on the **Camera** tab.

**Standard** mode image:




**Advanced** mode image:

© 2015




## Camera Policies Camera Tab Elements

This table includes both **Standard** and **Advanced** mode descriptions. Any **Advanced** mode features are noted as such.

| Element | Description |
|---|---|
| **Camera** | The Camera drop-down list displays all configured RTSP and VMS-managed cameras.<br>• Select a camera to be used for the policy. The available camera options following depend on the camera selected.<br>To add and configure a camera for use with multiple policies see add IP camera standard. |

| Element | Description |
|---|---|
| **Camera Type** | **Advanced mode only.**<br><br>The camera types can be an IP camera, a VMS-managed type of either Milestone managed camera, OnSSI managed camera, or exacq managed camera. |
| **Name** | A user defined value used in the menus and configuration file. This is the name of the camera.<br><br>The name entered is for identification purposes only. It is best to use a naming convention and a descriptive name. |
| **Description** | A user defined value used in the menus and configuration file. This is a description of the camera. |
| **Camera Pool** | **Advanced mode only.**<br><br>A camera pool is a user defined virtual grouping of cameras to search video from specified cameras. For example, suppose you have a camera pool called "Doors". It is comprised of all the cameras that watch over the doors of your business. When you need to see who's come or gone, select the "Doors" camera pool as a search criteria, and only video captured from this camera pool are included. There is no limit to the number of camera pools your Phoenix RSM solution may have. |
| **Manufacturer** | The manufacturer of the camera. The Video Capture URL populates automatically. |
| **Model** | A user defined value. This is the camera's model number. |
| **Video Capture URL** | The RTSP URL of the camera for capturing video feeds.<br><br>• The text box displays the IP address for the selected camera. |
| **User Name** | Type a User Name if the camera requires a user name and password to be accessed. This box works in conjunction with Password. |
| **Password** | Type a Password if the camera requires a user name and password to be accessed. This box works in conjunction with User Name. |
| **Alternative Frame Size** | **Advanced mode only.** |

© 2015

| Element | Description |
|---|---|
| | The width and height, in pixels, of video images. Use to define a frame size that is different from the camera's default. The first box is for width and the second is for height. |
| **Enable stream over TCP** | **Advanced mode only.**<br><br>Causes the RTSP capture to stream data over a TCP connection rather than over a default HTTP connection. |
| **Recording Computer** | Displays the computer that captures a video feed from your camera. |
| **Clip Duration** | **Advanced mode only.**<br><br>A video recording option.<br><br>Captured video feeds are parsed into individual files (default is 5 minutes). Use to select the size of these files and, therefore, the duration of individual videos.<br><br>Shorter videos (smaller files) enable the Surveillance Video Manager to retrieve files for review more quickly and causes the Information Repository to contain more files. Longer clips (larger files) mean fewer files. In either case, the amount of storage space used depends only on the amount of data that is captured, not the number of files. |
| **Cache Folder** | **Advanced mode only.**<br><br>A video recording option.<br><br>The cache folder is where incoming video streams are stored when they are first captured but not yet in the Information Repository.<br><br> Each camera should have its own cache directory.<br><br>• Leave the setting **Default Location** or select **At Pathname** and type the path. |

Additional Camera items for cameras managed by Milestone, OnSSI, or exacqVision:

| Element | Description |
|---|---|
| **Server Address** | The host name or IP address of the image server from extract video location. |

© 2015

| Element | Description |
|---|---|
| **User Name** | The user name who has rights to access the camera with video to extract. This must be a **Basic User**. |
| **Password** | If the camera requires a user name and password to be accessed, this is the password. This box works in conjunction with User Name. |

## Camera Policies Metadata Tab

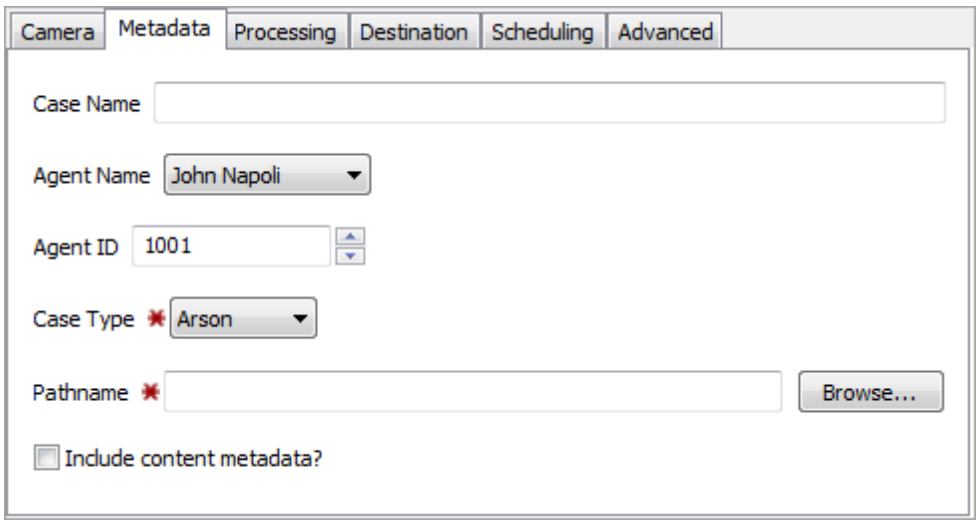
The Camera Policies **Metadata** tab is only displayed if it has been configured as described below.

Advanced users can create and configure an optional **Metadata** tab in the Camera Policies application and extended metadata search options in the Surveillance Video Manager. This is done by creating a text file called MetadataExtensions.cfg. With extended metadata you can ingest custom metadata that you want associated with videos. Later, when you need to find and retrieve videos, you can search using the extended metadata that was ingested when the video was processed.

The ingested metadata using Camera Policies is searchable using the Surveillance Video Manager. The metadata extensions for both applications are covered in MetadataExtensions.cfg.

The **Metadata** tab and metadata search options appear in the Camera Policies application and the Surveillance Video Manager only if there is a MetadataExtensions.cfg file in <install-dir>\Config.

The MetadataExtensions.cfg file must be on every computer where a recording policy could be modified, otherwise the metadata values could be lost.



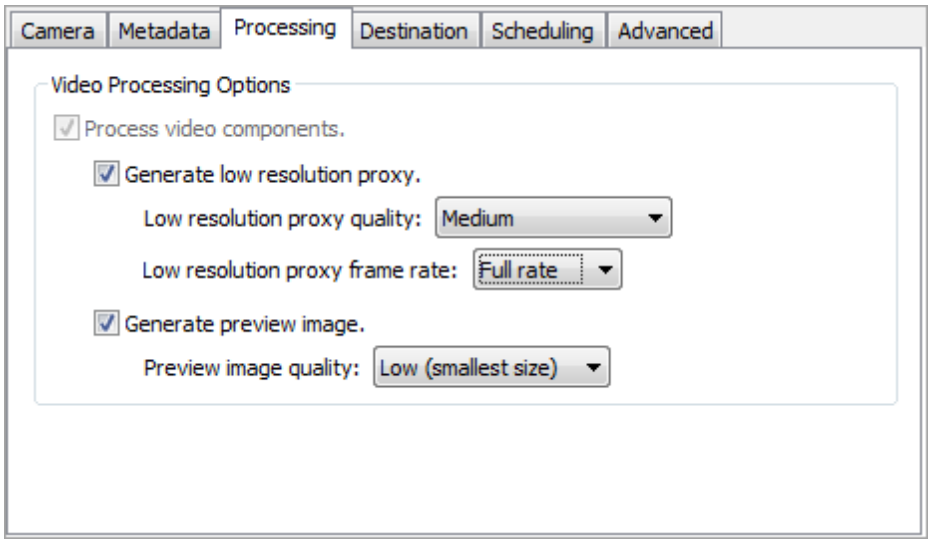

The red asterisk next to Case Type and Pathname mean that those are required fields.

© 2015

When you create, configure, and implement a MetadataExtensions.cfg file, the **Metadata** tab appears in Camera Policies. It contains the Query blocks listed in the IngestMdExt block.

## Camera Policies Processing Tab

Use the Camera Policies **Processing** tab to define file processing options for your recording policy. The contents on the **Processing** tab are the exact same as displayed in User Preferences. The preferences entered in at the **Processing** tab override any defaults that may be set in the User Preferences window, but only for the current job or policy. This tab only displays if you are in Advanced mode.




For more information see Camera Policy User Preferences.

### Video Processing Options

Use these options to capture video files for viewing. Elect to generate low resolution companion videos (also called proxy files) or preview images during video capture. The low resolution proxies and preview images have a relatively small file size which make it quick and easy to search for video files and clips without having to wait for the retrieval of large, original video files.

The **Process Video Components** checkbox is selected by default and cannot be de-selected.

| Elements | Description |
|---|---|
| **Generate low resolution proxy** | 1. Select to generate low resolution companion files. If not selected, the proxies are not created, but you can always view the original video in the Information Repository.<br><br>The low resolution file is a fraction of the size of the original video size. When searching for video, the low resolution video is the primary video footage received but it is always paired with the original source video. The original (stored either online, near-line, or offline) is totally accessible when needed and under full Phoenix RSM management. |

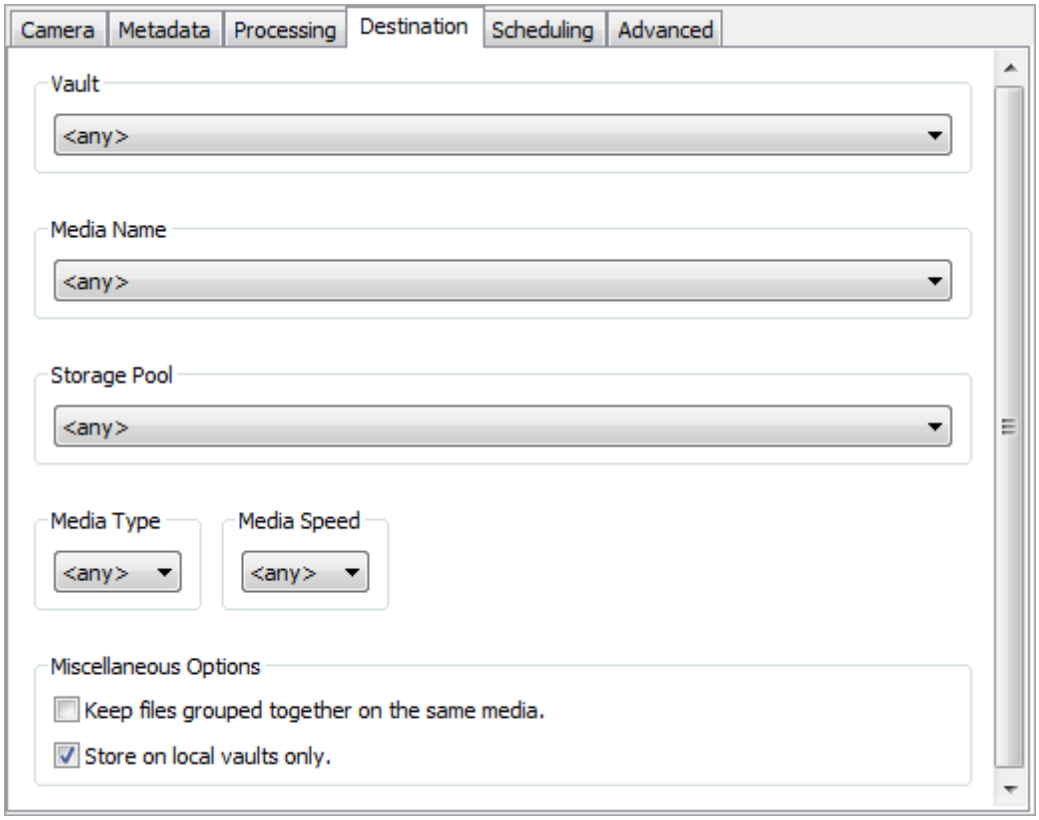
© 2015

| Elements | Description |
| --- | --- |
| | 2. Select a resolution quality setting for the proxy/companion video. A lower setting produces a smaller file.<br>• **High** - Same frame size as original, high video quality, audio is compressed to QDesign 44kHz.<br>• **Medium** - 320x240 frame size, medium video quality, audio is compressed to QDesign 44kHz.<br>• **Low** - 320x240 frame size, low video quality, audio is compressed to QDesign 14kHz.<br>3. Select a frame rate for the low resolution/companion video.<br> Phoenix RSM will not generate thumbnails or low resolution proxies for files. |
| **Generate preview image** | 1. Select to generate a preview image; if not selected a preview image is not created.<br>2. Use the **Preview image quality** drop-down list to select a resolution setting. A lower setting produces a smaller file.<br>• **High** - Original size.<br>• **Medium** - 320x240.<br>• **Low** - 100x75. |

© 2015

## Camera Policies Destination Tab

Use the Camera Policies **Destination** tab to determine the Vaults, media, storage pools, and other options where your video files are recorded or captured. Read this section before you set Vault, Media Name, Storage Pool, Media Type, and Media Speed parameters. This tab only displays if you are in Advanced mode.




Only the default names of <any>, <unnamed>, <new entry>, or implemented names of Vaults, storage pools, media, media types, and media speeds already in the Information Repository appear in the **Destination** tab drop-down lists. New names with associated parameters appear also, once added.

You can enter names of new Vaults, media, or storage pools to the Information Repository before actually adding them, the names will appear beneath <any> in the given field. However, it is recommended to select only media that appears in the drop-down list, otherwise you may increase chances of error.

There are several options for populating the **Destination** tab fields:

- **Leave the default values (<any>)** - Phoenix RSM determines the most accessible Vault and the media with the most free space.
- **Select a parameter and let Phoenix RSM take care of the rest** - For example, if the Media Speed of S8 is selected, then only media running at the speed associated with S8 writes. Or, if Storage Pool or Media Name is selected, then files are only sent to the storage pool or media selected. With a selected Vault, Phoenix RSM uses the most available Vault or media with the most free space.

© 2015

- **Select a parameter and select available parameters from remaining fields** - If a Vault, Media Name, or Storage Pool parameter is selected, then remaining fields have limited options available which correspond to the parameter.

To reset the **Destination** tab with all parameters from any field, select **<any>** in the **Vault** group.

Several units of media can be assigned to a single storage pool. See Prepare Media - Storage Pool.

- **Create a new entry for a Vault, Media Name, or Storage Pool** - From the Vault, Media Name, or Storage Pool drop-down list, select **<new entry>**. The Enter New Name window appears for you to type a new name. Click **OK** and the new entry appears in the field's drop-down list.

This method is recommended only for special circumstances. If a job is run with a Vault or media that is not actually running in the Information Repository, the job fails.

The <any> item in the drop-down list also acts as a divider between Vault, media, and storage pools implemented and those not implemented. Names above <any> are the ones running in your Information Repository, and the names below <any> are entered but do not yet have hardware implemented in the Information Repository. These are not saved if not selected when saving the policy.

The limitations to adding a new name for a Vault, Media Name, or Storage Pool are:

- Typing a new name for the Vault, Media Name, and Storage Pool options are limited to <any> and <new entry>.
- New entries in Media Name or Storage Pool do not limit options in the remaining fields.
- Wildcard additions (for example, Ac*), appear beneath <any>. See Wildcards.

## Camera Policies Destination Tab Elements

| Element | Description |
|---|---|
| **Vault** | From the drop-down list select a Vault, or select **<new entry>** to add a new Vault name. The Enter New Vault Name window opens for you to type a Vault name.<br><br>If a Vault is selected, the Media Name drop-down list is automatically populated with the media on the given Vault.<br><br>If a new entry is given, then the Media Name and Storage Pool options are limited to <any> or <unnamed> and <new entry>. |
| **Media Name** | Media Name refers to the names of individual units of media in the Vaults within the Information Repository. |

© 2015

| Element | Description |
|---|---|
| | From the drop-down list select the media, or select **<new entry>** to add a new media name. The Enter New Media Name window opens for you to type a media name. The system automatically looks for any storage pools comprised of the selected media. If it cannot find any, then the Storage Pool drop-down list displays <any>. |
| **Storage Pool** | Storage pools are groupings of media on a single policy used for a particular purpose. For example, if you had a policy called "Night backup" and it wrote to several units of media, you would use a "Night backup" storage pool and assign to it every unit of media to use for that purpose. For more information see Prepare Media, Storage Pool.<br><br>From the drop-down list select a storage pool, or select **<new entry>** to add a new storage pool name. The Enter New Storage Pool Name window opens for you to type a name. |
| **Media Type** | Determine the types of media a policy uses by specifying a media type. For example, if "Hdisk" is selected, then only Hdisk media is used. Media Type is useful for processing data of lower importance or less rigorous recovery time objectives.<br><br>From the drop-down list select the media type. Only media types for the parameters selected in the Vault, Media Name, or Storage Pool drop-down lists are displayed. If none were selected, then only the media types from media available within the Information Repository are displayed.<br><br>Set either Media Type or Media Speed, but not both. |
| **Media Speed** | Source files run based on speed and media performance. This is useful for processing data of lower importance or less rigorous recovery time objectives.<br><br>Hard disk is considered a high performance media and is assigned a high rating of (S8). Slower data tape technologies are lower performance and are assigned a lower rating of (S0).<br><br>From the drop-down list select a performance rating. Only media speeds for the parameters selected in the Vault, Media Name, or Storage Pool drop-down lists are displayed. If none were selected, then only the media speeds from media available within the Information Repository are displayed.<br><br>Set either Media Type or Media Speed, but not both. |

© 2015

| Element | Description |
|---|---|
| **Miscellaneous Options** | Select **Keep files grouped together on the same media** to have Phoenix RSM write files to the same media. If de-selected, targeted files store across the Information Repository on whatever media has the most space and best availability.<br><br>Select **Store on local Vaults only** to store files on the host computer where the policy lives. |

### Offline Media

When videos are being captured, offline media are never used as a destination, even if offline media is selected, it is not used. Attempting to use media that is offline may result in a “No resources available” error.

## Camera Policies Scheduling Tab

Use the Camera Policies **Scheduling** tab to define when to record video from your RTSP-enabled IP camera or when to capture from your VMS-managed camera. You can record or capture video always or on a daily basis. As soon as you save the given policy, the schedule you created is implemented.

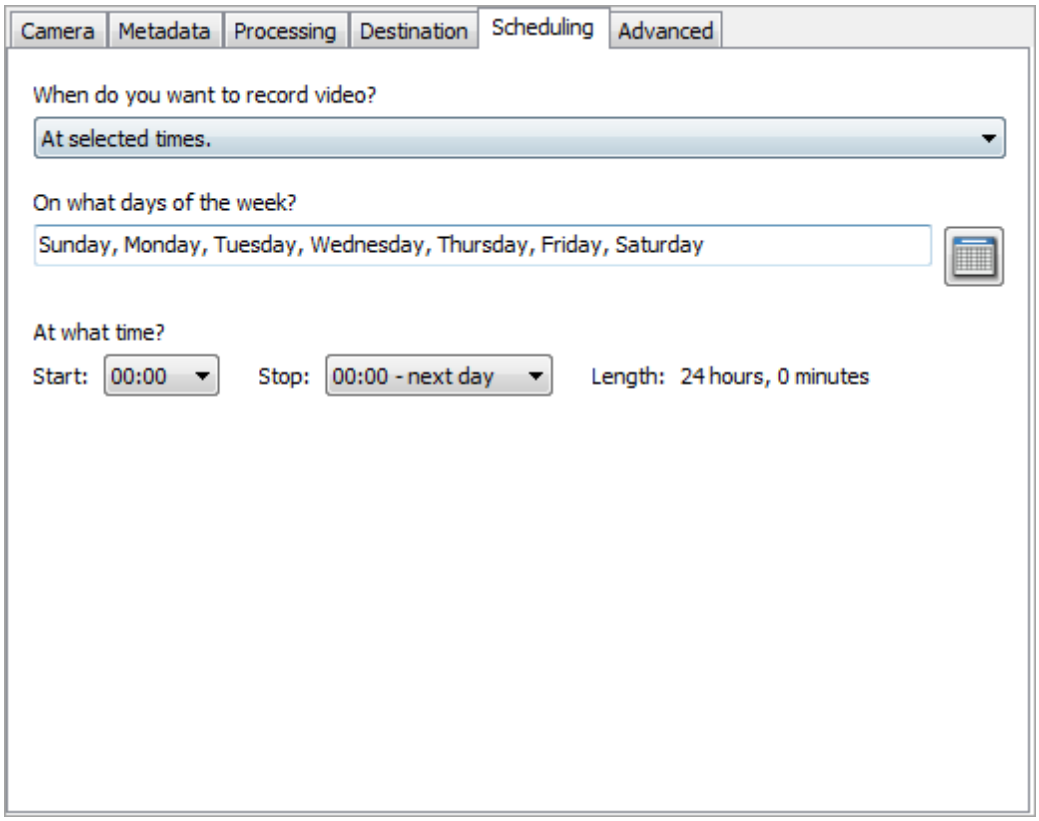
### Scheduling a Job for Recording or Capturing Video

The **Scheduling** tab displays different fields to populate depending on the parameter set for the **When do you want to record video?** option. Select an option to define the times when video is recorded or captured.

From the **When do you want to record video?** drop-down list, select one of the options to schedule a process. Each are described below.

- Option 1: Always
- Option 2: At Selected Times

© 2015




### Always

This option enables you to record or capture video 24 hours a day, seven days a week for as long as the policy is active. To stop a policy that has been set to record video always, you must deactivate, change, or delete the policy. When you select this option, the rest of the **Scheduling** tab fields are inactive.

### At Selected Times

This option enables you to schedule video recording or capture on particular days at specific times.

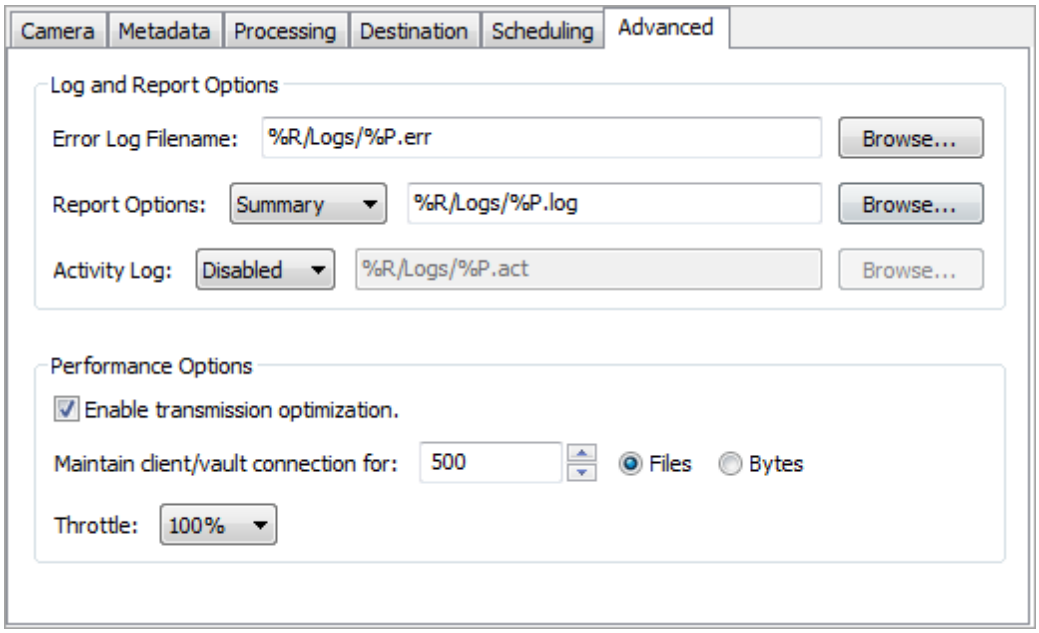
1. For the **On what days of the week?** text box, click the **Calendar** button. This opens the Days window to select the days of the week to record or capture video.
2. For the **Start time** drop-down list, select a start time.
3. From the **Stop** drop-down list, select a stop time.

Once you have selected start and stop times, the **Length** element displays the total number of hours that video is to be recorded or captured per day.

© 2015

## Camera Policies Advanced Tab

Use the Camera Policies Advanced tab to set log, report, and performance options. This tab only displays if you are in Advanced mode.




### Camera Policies Advanced Tab Elements

| Element | Description |
|---|---|
| **Error Log Filename** | An error log file is created anytime an error is encountered during a job. It is useful for troubleshooting problems. The **Error Log Filename** text box can include literal file names or a combination of file name field variables to generate file names for logs.<br>• Leave the default variables in place, or type in a file name and extension to use, or type in a variable name using file name field variables (see **File Name Field Variables** section below).<br>• Use the **Browse** button to define a new location and type in the file name that you want to use, including an extension. |

© 2015

| Element | Description |
|---|---|
| **Report Options** | When a job runs, one of the following report files is created:<br>**Summary** - A header and summary report<br>**Complete** - Same as summary and lists all files<br>**Diagnostic** - Same as complete, but adds relevant diagnostic information<br>• From the drop-down list select a report option. Use the **Summary** or **Complete** options on a normal basis and switch to **Diagnostics** if problems occur.<br>• In the **Report Options** text box, leave the default variables in place, or type in the file name and extension to use, or type a variable name using file name field variables (see **File Name Field Variables** section below).<br>• Use the **Browse** button to locate a file to overwrite an already existing log file. |
| **Activity Log** | Activity logs provide logistical information about jobs. Refer to the logs after a job runs; they are stored in a specified location.<br>• Set **Activity Log** to **Enabled**. The Activity Log text box becomes active.<br>• In the **Activity Log** text box, leave the default variables in place. Or, type in a file name to use, including an extension. Or, type in a variable name using **Filename Field Variables** (see section below).<br>• Opt to use the **Browse** button to define a new location and type in the file name. |
| **Enable Transmission Optimization** | Select for the client to constantly monitor its processes and to determine the best network transmission protocol for files being processed. Leave this option selected to get up to a 20% increase in performance. If the Information Repository is slow, run a few timed tests to determine a setting that works best for your Information Repository. |

© 2015

| Element | Description |
|---|---|
| **Maintain Client/Vault Connection** | Vault connection sharing determines how many files are sent from the source Vault to the destination Vault in a single connection. The higher the number of files or bytes transferred, the longer the connection between the source and destination Vault is maintained. Access to a particular Vault resource (such as one drive of a multi-drive storage device) used by a process on one client is restricted and inaccessible to other clients in the network for the duration of the connection.<br><br>To illustrate this, imagine an environment where a single Vault with a single tape drive is used to service several desktop clients. When a client is configured with a connection sharing set to 250 files and other clients are configured to start jobs at the same time, no client can connect until the first client is finished. Each connection to the server locks out other connections and other clients must wait before processing files.<br><br>1. Type an integer value into the **Maintain Client/Vault Connection for** text box.<br><br>2. Select the **Files** radio button or **Bytes** radio button. By selecting Files, a connection sharing proceeds based on the number of files transmitted or if Bytes, based on the number of bytes. |
| **Throttle** | The throttle controls the speed that files are sent to the Vault. Lower numbers reduce the bandwidth. Throttle values range from 10% to 100% of total available bandwidth.<br><br>• From the **Throttle** drop-down list, select a percentage to operate the client on its host computer for maximum performance.<br><br>Phoenix RSM is designed to operate at maximum performance of its host computer, network environment, and storage resources available. During normal working hours, running a job at peak performance could interfere with other network operations. |

© 2015

### File Name Field Variables

The file path can include a literal file name or a combination of variables to generate file names for reports. Use variables to distinguish between reports and to find specific reports.

If a path with a literal file name is typed like C:/Program Files/Logs/Job_Report.log, the system generates the report destination folder Logs (if it does not already exist) and a report named Job_Report.log. If a path with variables for the file name is typed, for example, %R/Logs/%P_from_%H_on_%D_at_%T, the system generates the report destination folder and a report — where policy name, host name, date, and time are populated with the actual details from your Information Repository and job.

The following are the variables to use. When using multiple variables, separate them from each other with an underscore (_).

| Variable | Description |
|---|---|
| %P or %Pn | Policy Name |
| %H or %Hn | Host Name |
| %D | Date (yyyy:mm:dd) |
| %Dy | Year |
| %Dm | Month |
| %Dd | Day |
| %T | Time (hh:mm) |
| %Th | Hour |
| %Tm | Minute |
| %Ts | Second |
| %R or %Rn | Root Pathname. Valid only at the beginning of a string |

## Camera Policies User Preferences

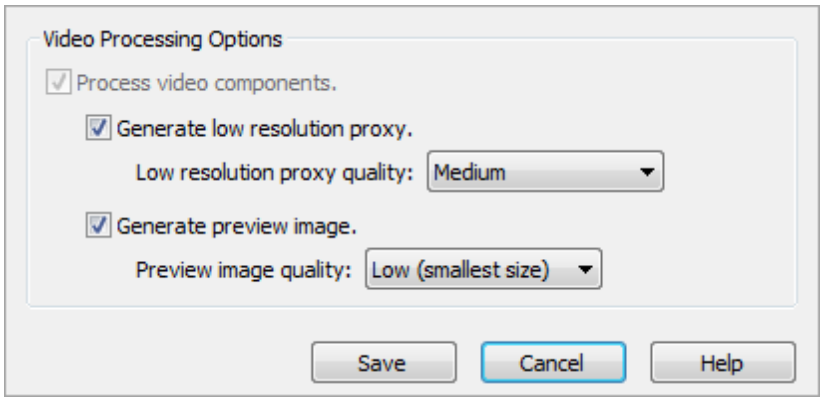
User Preferences define default settings for Camera Policies. The information in User Preferences is the exact same as what is displayed on the Processing tab. The User Preferences entered become the defaults for the application. Changes made on the **Processing** tab override settings in User Preferences, but only for the given job or policy.

Refer to the Camera Policies Processing Tab Elements section for details about the **User Preferences** options.

Preferences are an excellent way to streamline projects, providing a convenient way to set commonly used options for your desktop client. Each subsequent time you run a job using your desktop client, those settings are automatically set.

© 2015

Access the User Preferences from the Camera Policies **Tools** menu, select **User Preferences**.




### Camera Policies User Preference Elements

#### Video Processing Options

Use these options to capture video files for viewing. Elect to generate low resolution companion videos (also called proxy files) or preview images during video capture.

The **Process Video Components** checkbox is selected by default and cannot be de-selected.

| Elements | Description |
|---|---|
| **Generate low resolution proxy** | Select to generate low resolution companion files.<br>From the **Low resolution proxy quality** drop-down list, select a resolution quality of **High**, **Medium**, or **Low**.<br>From the **Low resolution proxy frame rate** drop-down list, select one of the listed frame rates. |
| **Generate preview image** | Select to generate a preview image.<br>From the **Preview image quality** drop-down list, select a resolution quality of **High**, **Medium**, or **Low**. |

## Camera Configurations

View live feeds from RTSP-enabled IP cameras and record video directly from RTSP-enabled IP cameras. To do this, you need to add cameras to your Information Repository and configure them. Once added, the cameras are listed on the **Camera** tab of every Camera Policies application on your network.

The first step is to add a camera configuration using SoleraTec's Phoenix RSM Camera Policies application.

To record video from a RTSP-enabled IP camera, the quickest and easiest way to do it is to use the Add Camera Wizard. Sometimes you may need to capture video from a VMS-managed camera or edit existing cameras configurations - this is done through the Camera Configurations window.

© 2015

Use Camera Configurations:

- To view a list of all the configured cameras that have been created and are available for recording.
- To modify existing camera configurations.
- For manually adding VMS-managed (Milestone, OnSSI, or exacqVision) cameras to create policies to capture video into the Information Repository.
- For manually adding cameras where the camera manufacturer or model are not found on the network.

## Add New Cameras

To add a camera through Camera Configurations, see Manually Add IP Camera or Add VMS Camera.

## Modify Camera Configurations

To modify an existing camera configuration:

1. From the Camera Policies toolbar, click the **Cameras** button. This opens the Camera Configurations window populated with a list of all of the cameras configured in the Information Repository.
2. Select the camera to modify from the list.
3. From the Camera Configurations menu, select **Edit** > **Modify Selected Camera**. The Modify Camera window opens and is populated with camera parameters for the selected camera.
4. Change the options and values as needed and then click **OK**.
5. From Camera Configurations, click the **Save** button to save the modified camera.

For easy access to the Modify Camera Window, from the Camera Configurations camera list, right-click a selected camera and select **Edit**.

## Delete Camera Configurations

To delete an existing camera configuration:

1. From the Camera Policies toolbar, click the **Cameras** button. This opens the Camera Configurations window, populated with a list of all of the cameras configured in the Information Repository.
2. Select the camera to delete from the list.
3. Click the Delete button.
4. If you are certain to delete the camera configuration from Information Repository, in the Confirmation window, select **Yes**. The camera is deleted from your Information Repository and from the list in the Camera Configurations window.

© 2015

5. From Camera Configurations, click the **Save** button to save the modified camera configurations.

To easily delete a camera, from the Camera Configurations camera list, right-click a selected camera and select **Delete**.

To delete all camera configurations:

1. From the Camera Policies main menu, select **Tools** > **Cameras**. This opens the Camera Configurations window, populated with a list of all of the cameras configured for your system.
2. From the Camera Configurations main menu, select **Edit** > **Delete All Cameras**.
3. If you are certain you want to delete all camera configurations from your entire Information Repository, in the Confirmation window, select **Yes**.
4. From Camera Configurations, click the **Save** button to save changes.

## Camera Configurations Window

The Camera Configuration window displays a list of the camera configurations that have been created and are available for use by recording policies.

The column headings displayed in Camera Configurations are Camera Name, Manufacturer, Model, Video Capture URL, Status, Camera Pool, Recording Computer, and Description.

The Camera Configurations toolbar consists of the following buttons:

- Save all configurations.

- Add a new camera configuration. See Manually Add IP Camera or Add VMS Camera.

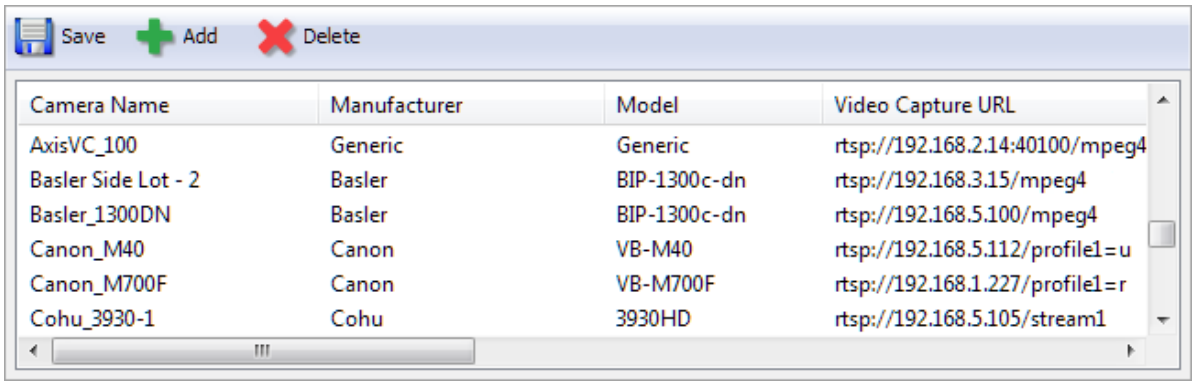
- Delete a camera configuration.

You can always edit an existing camera configuration. From the Camera Configurations window select an individual configuration, right-click, and select **Edit** from the shortcut menu. This shortcut menu also features **View Live** - where you can review a live video feed in a viewer, **Manage** - where you can view the video feed in a Web browser (URL from the camera manufacturer), **Change Active Setting** - where you can choose for the camera to be active or inactive, **Set Recording Computer** - where you can select the computer that captures the camera video feed, and **Delete** - to remove the camera from the list of configurations.

When changing the **Active Setting** or **Recording Computer**, you can also select multiple configurations by holding the**Shift** key or the **Control** key and clicking on the desired configurations.

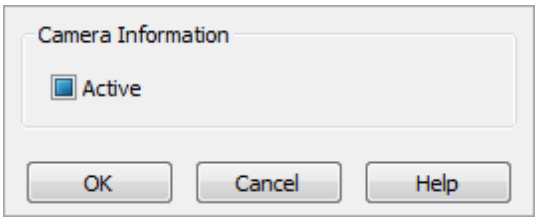
To view and record live video feeds, ensure the RTSP is enabled on your IP camera. See your camera's documentation for details on enabling RTSP.

© 2015



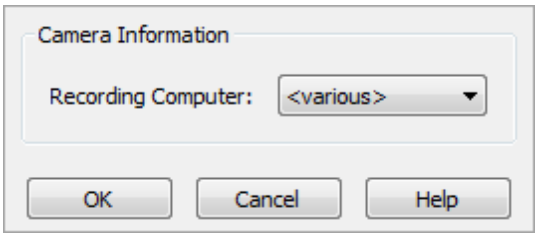

**Change Active Setting** - To capture video and view live feeds, this checkbox must be selected. If it is not selected, then any policy that uses this camera will not run.

When multiple configurations are selected with different current active settings, the checkbox will be shaded to indicate the selected configurations have different **Active Settings**.




**Set Recording Computer** - Use the drop-down menu to select a computer which will capture the video feed for the selected configurations. You can also choose for no **Recording Computer** to be used by selecting the option **<not selected>**.

When multiple configurations are with different **Recording Computers** currently selected, **<various>** will be shown to indicate that different **Recording Computers** are currently being used for the selected configurations.




## Camera Configurations Menu Items

| Menu Items | Description |
|---|---|
| **File > Save All** | Save settings for camera configurations created or modified. |

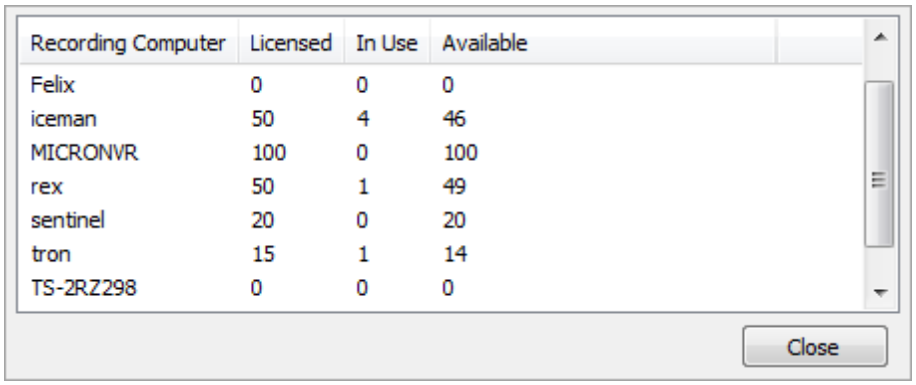
© 2015

| Menu Items | Description |
|---|---|
| **File > Import from** | Open an Import from window to select a camera configuration file that contains values for the configuration. |
| **File > Export to** | Open an Export to window to select where a camera configuration file saves to. |
| **File > Exit** | Close the application. If changes have been made a Confirmation dialog box appears for saving changes, click **Yes**, **No**, or **Cancel**. |
| **Edit > Add a Camera** | Open the Add New Camera window. Depending on whether you are working in Camera Policies **Standard** mode or **Advanced** mode, this window displays a shortened or expanded view of options, respectively.<br><br>Manually enter camera information for the new configuration. See Manually Add IP Camera. |
| **Edit > Modify Selected Camera** | Open the Modify Camera window to change existing values entered for camera information. |
| **Edit > Delete Selected Camera** | Remove the selected camera from the Camera Configurations list. |
| **Edit > Delete All Cameras** | Remove all cameras listed in the Camera Configurations window. |
| **Tools > Camera Allocation** | Open the Camera Allocation window. Use to glance at the basic configuration of your cameras, such as, cameras licensed, cameras in use, and recording computer camera availability. |
| **Help > Current Page** | Open online help to the Camera Configurations webpage. |
| **Help > About Camera Policies** | Open the About Camera Policies window. |

## Camera Allocation

In the Camera Configurations window, from the **Tools** menu, select **Camera Allocation**. This is an informational window to show how many cameras are licensed, how many cameras are being used, and how many cameras are available for each recording computer. Use this information to manage and change where cameras are allocated using functions in the Camera Configurations window.

© 2015




**Import/Export Camera Configurations**

You can import or export camera configuration files. This section details the format of the file that is created whenever you export camera configurations from Camera Policies. While it is best to use Camera Policies to change your camera configurations, you can also do so by creating and importing a special file.

The procedures for exporting and importing a camera configurations file are below - they are geared towards advanced users.

## Export Current Camera Configurations to a File

1. From the Camera Policies main menu, select **Tools** > **Cameras**. The Camera Configurations window appears.
2. From the Camera Configurations main menu, select **File** > **Export to**. The Export to window appears. The default file name is Cameras.cfg.
3. Navigate to the location to export the file, and then click **Save**. The file is saved to the location you selected.

## Import a Configuration From a File

1. From the Camera Policies main menu, select **Tools** > **Cameras**. The Camera Configurations window appears.
2. From the Camera Configurations main menu, select **File** > **Import from**. The Import from window appears.
3. Navigate to the file location where you have saved your camera configurations file, select it, and then click **Open**. The camera configurations from the file are added to the Camera Configurations window.
4. Click the **Save** button to save the modified camera configurations to your Information Repository.

Before you can import a camera configuration file, you must create one. The following sections contain reference information for doing so.

© 2015

## Camera Configuration File Structure

Camera configuration files are block structured but free from any column or order formatting. The tokens listed below specify camera parameters. Each "policy_name" block is a single camera.

```
policy_name="<camera name>"
[
    <token>=<value>
    <token>=<value>
    . . .
]
policy_name="<camera name>"
[
    <token>=<value>
    <token>=<value>
    . . .
]
. . .
```

## Tokens/Value Pairs

Tokens define camera attributes and functionality. Following are the tokens and their definitions.

| Token/Value | Description |
|---|---|
| ace = data | The access control list entry.<br>No default. |
| active = <*boolean*> | Determine if the camera is active or inactive. For the live view and camera management to work, this option must be set to true.<br>Valid values: true \| false<br>Default = true |
| description = "<*character string*>" | A description of the camera.<br>Default = "" |
| frame_height = <*integer*> | The height of the video frame. Works in conjunction with frame_width.<br>Default = 0 |
| frame_width = <*integer*> | The width of the video frame. Works in conjunction with frame_height<br>Default = 0 |

© 2015

| Token/Value | Description |
|---|---|
| host_Id = "<*uuid*>" | The host Id of the recording computer.<br>Default = 0 |
| hostname = "<*character string*>" | The host name of the recording computer.<br>Default = "" |
| live_view_enable = <*boolean*> | Enable SVM to receive and display live feeds from the camera.<br>Valid values: true \| false<br>Default = true |
| live_view_url = "<*pathname*>" | The RTSP URL used to live view video from the camera.<br>Default path = "" |
| manufacturer = "<*character string*>" | The manufacturer of the camera.<br>Default = "Generic" |
| mgmt_enable = <*boolean*> | Enable camera management from a web browser when this type of functionality is supported by the camera.<br>Valid values: true \| false<br>Default = true |
| mgmt_url = "<*URL*>" | The URL used to manage the camera.<br>Default URL = "" |
| model = "<*character string*>" | A user defined value, this is the camera's model number.<br>Default = "Generic" |
| name = "<*character string*>" | Must match the "policy_name".<br>The name of the camera.<br>Default = "" |
| owner = "<*character string*>" | Internal use only. |
| password = "<*character string*>" | The password for the camera when a password is required to access the camera. |

© 2015

| Token/Value | Description |
|---|---|
| | Default = "" |
| policy_name = "<*camera name*>" | Must match "camera_name".<br>Indicating the beginning of a camera block, the name for the policy that defines camera parameters.<br>Default = "" |
| pool = "<*character string*>" | The name of the camera pool.<br>Default = "" |
| ptz_enable = <*boolean*> | "PTZ" stands for "pan, tilt, zoom." Use to set the pan, tilt, and zoom functionality for the camera. For PTZ to work, this option must be selected.<br>Valid values: true \| false<br>Default = true |
| stream_over_tcp = <*boolean*> | Cause the RTSP capture to stream data over a TCP connection rather than over a default HTTP connection.<br>Default = false |
| thumbnail_url = *"<pathname>"* | The HTTP URL for producing images.<br>Default = "" |
| thumbnail_enable = <*boolean*> | Enable the thumbnail URL.<br>Valid values: true \| false<br>Default = false |
| type = "<*character string*>" | The policy type of the file.<br>Default = "camcfg" |
| user_name = "<*character string*>" | The user name of the camera when a user name is required to access the camera.<br>Default = "" |
| version = <*number*> | The version number of the policy. The current version is 1.0. |

© 2015

| Token/Value | Description |
|---|---|
| video_capture_lrp_url = *"<pathname>"* | The RTSP URL for capturing low resolution video feeds.<br>Default = "" |
| video_capture_lrp_enable = <*boolean*> | Enable the video capture LRP URL.<br>Valid values: true \| false<br>Default = false |
| video_capture_url = "<*url*>" | The RTSP URL used to capture video from the camera.<br>Default = "" |
| vms_lrp_create = <*boolean*> | Enable the VMS (Milestone or OnSSI) to generate the LRP.<br>Valid values: true \| false<br>Default = true |
| vms_rec_mot_detect = <*boolean*> | Enable record on motion detection.<br>Valid values: true \| false<br>Default = false |
| vms_rec_mot_threshold_sec = <*integer*> | The motion detection threshold.<br>Default = 5 |

### Sample Cameras.cfg File

```
policy_name = "Panasonic_sp306"
[
    type                    = "camcfg"
    version                 = "1.0"
    active                  = true
    name                    = "Panasonic_sp306"
    description             = ""
    model                   = "WV-SP306"
    manufacturer            = "Panasonic"
    pool                    = ""
    user_name               = "admin"
    password                = "12345"
    video_capture_url       = "rtsp://192.168.5.103/MediaInput/h264"
    live_view_url           = "rtsp://192.168.5.103/MediaInput/h264"
    mgmt_url                = "http://192.168.5.103/"
```

© 2015

```
    frame_width             = 0
    frame_height            = 0
    ptz_enable              = true
    live_view_enable        = true
    mgmt_enable             = true
    stream_over_tcp         = false
    owner                   = ""
    host_Id                 = "00000000000000000000000000000000"
    hostname                = ""
    ace                     = "0008001901010800"
]
# end of object rule for Camera 'Panasonic_sp306'

policy_name = "SecureEye-1080"
[
    type                    = "camcfg"
    version                 = "1.0"
    active                  = true
    name                    = "SecureEye-1080"
    description             = "StoreNet SecureEye"
    model                   = "SecureEye-1080p-IP"
    manufacturer            = "StoreNet"
    pool                    = ""
    user_name               = "admin"
    password                = "1"
    video_capture_url       = "rtsp://192.168.1.244/stream1"
    live_view_url           = "rtsp://192.168.1.244/stream1"
    mgmt_url                = "http://192.168.1.244/"
    frame_width             = 0
    frame_height            = 0
    ptz_enable              = true
    live_view_enable        = true
    mgmt_enable             = true
    stream_over_tcp         = true
    owner                   = ""
    host_Id                 = "31b1d2b5c44111e0af6200132051d593"
    hostname                = "tron"
    ace                     = "0008001901010800"
]
# end of object rule for Camera 'SecureEye-1080'

policy_name = "Sharx"
[
    type                    = "camcfg"
    version                 = "1.0"
    active                  = true
    name                    = "Sharx"
    description             = "SCN2607"
    model                   = "SCNC2607"
    manufacturer            = "Sharx"
    pool                    = ""
    user_name               = "admin"
    password                = "admin"
```

```
    video_capture_url        = "rtsp://192.168.5.242/live_mpeg4.sdp"
    live_view_url            = "rtsp://192.168.5.242/live_mpeg4.sdp"
    mgmt_url                 = "http://192.168.5.242/"
    frame_width              = 0
    frame_height             = 0
    ptz_enable               = true
    live_view_enable         = true
    mgmt_enable              = true
    stream_over_tcp          = false
    owner                    = ""
    host_Id                  = "00000000000000000000000000000000"
    hostname                 = ""
    ace                      = "0008001901010800"
]
# end of object rule for Camera 'Sharx'
```

## Manually Add IP Camera

For the most streamlined and efficient work flow, add your RTSP-enabled IP camera using the Add Camera Wizard. There are times, however, to add an IP camera manually, such as when your camera manufacturer and model cannot be found on the network.

Camera Policies hosts two modes, **Standard** mode and **Advanced** mode. When adding a camera configuration, the Add New Camera window appears with **Standard** mode options or with extended **Advanced** mode options, depending on which mode is enabled under the Camera Policies **View** menu. The following are procedures that take into account both modes and any differences are noted.

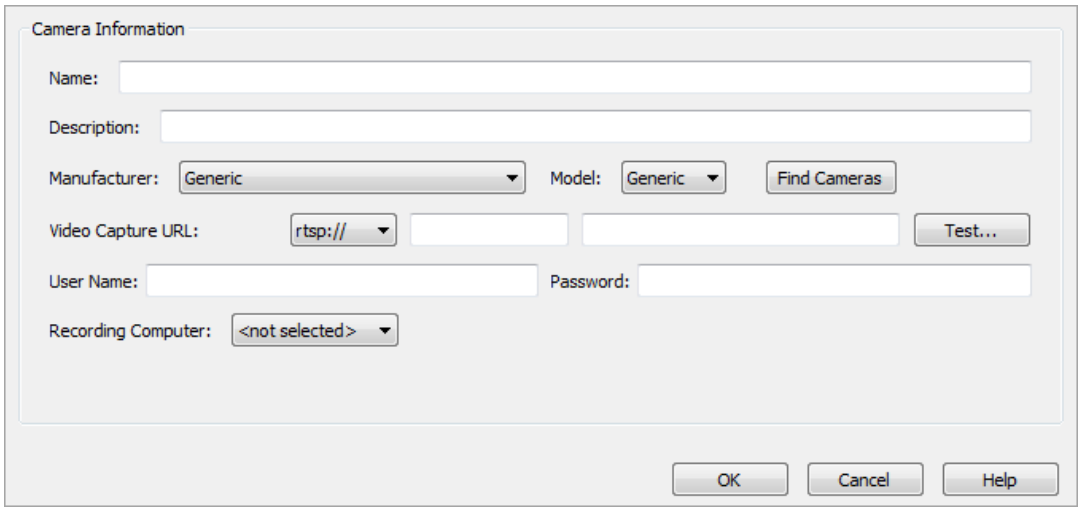
### To add a RTSP-enabled IP camera manually

1. From the Camera Policies toolbar, click the **Cameras** button to open the Camera Configurations window.

2. From the Camera Configurations toolbar, click the **Add** button. Or from the Camera Configurations main menu, select **Edit** > **Add a Camera**. The Add New Camera window displays differently depending on whether you are working in **Standard** mode or **Advanced** mode.

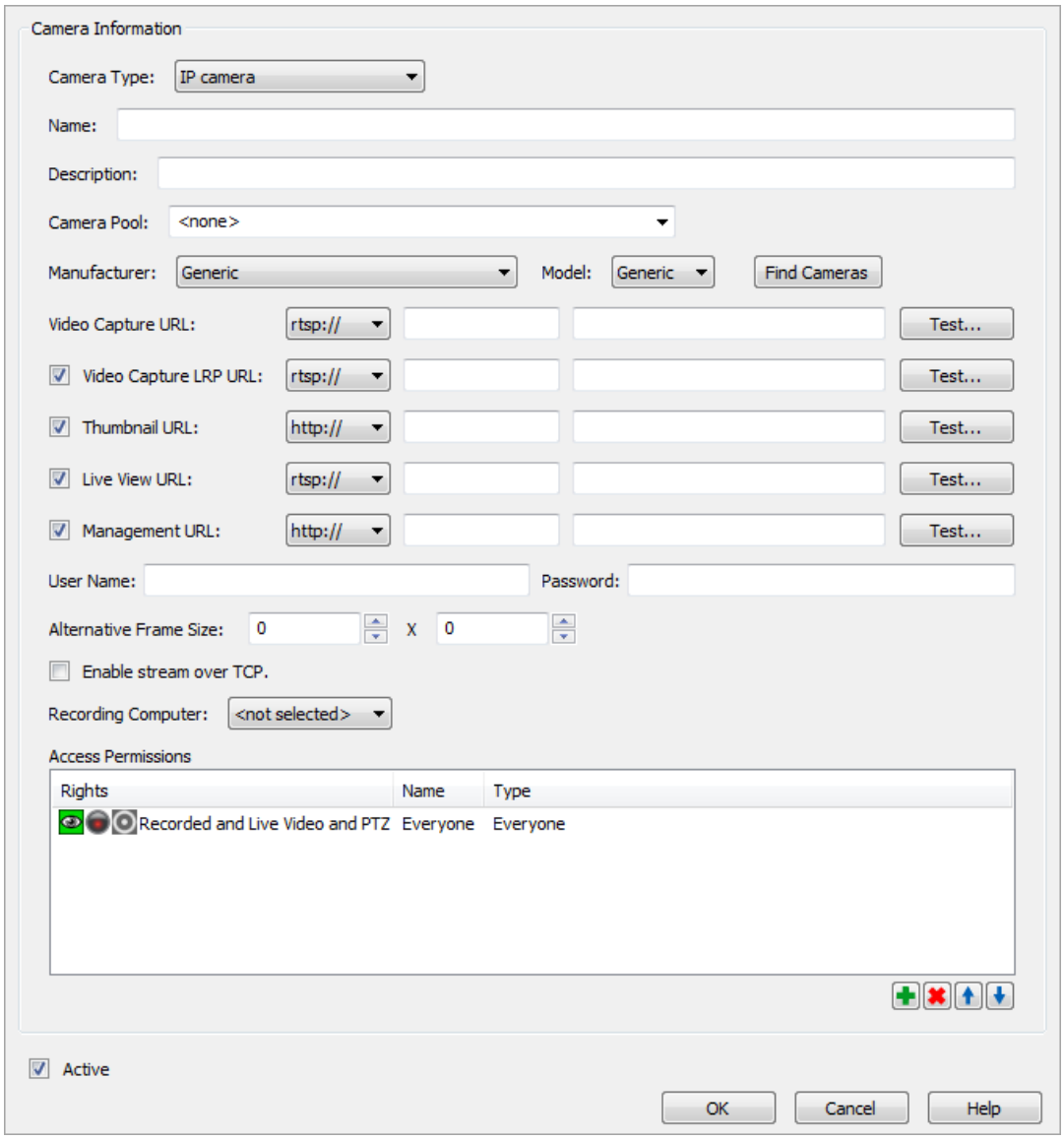
   **Standard** mode image:

© 2015




**Advanced** mode image:

© 2015




3. Populate the Add New Camera boxes appropriately for your camera. Some of the more advanced parameters allow you to specify a camera pool, an alternative frame size, or access permissions.

   Use the table below to help fill in the boxes.

| Element | Description |
|---|---|
| **Camera Type** | **Advanced mode only**.<br><br>The camera types can be an IP camera or a VMS-managed type of either Milestone managed camera, OnSSI managed camera, or exacq managed camera. |

| Element | Description |
|---|---|
| | If your camera is managed by a Milestone, OnSSI, or exacqVision video management system, see Add VMS Camera. |
| **Name** | Type a name used for menus and the configuration file, this is the name of the camera.<br><br>The name entered is for identification purposes only. It is best to use a naming convention and a descriptive name. |
| **Description** | Text used for defining the camera in menus and the configuration file. This is a description of the camera. |
| **Camera Pool** | **Advanced mode only**.<br><br>For the camera pool, define a virtual grouping of cameras to search video from specified cameras. For example, suppose you have a camera pool called "Doors". It is comprised of all the cameras that watch over the doors of your business. When you need to see who's come or gone, select the "Doors" camera pool as a search criteria, and only video captured from this camera pool are included. There is no limit to the number of camera pools your Phoenix RSM solution may have. |
| **Manufacturer** | Define the manufacturer of the camera. The Video Capture URL populates automatically. Click the **Find Camera** button for a listing of cameras found on the network. See Search Results window. |
| **Model** | Define the camera's model number. Click the **Find Camera** button for a listing of cameras found on the network. See Search Results window. |
| **Video Capture URL** | The RTSP URL of the camera for capturing video feeds. From the drop-down list, choose **rtsp://**.<br><br>• In the first text box type the IP address for the selected camera. The second text box populates automatically when a known camera manufacturer and model are selected.<br><br>• Click the **Test** button to test the RTSP URL. If the test is successful a Live View window appears. A successful connection should take no more than 10 seconds. If the test fails try the following: |

© 2015

| Element | Description |
|---|---|
| | i. Every camera has a RTSP URL. Validate the RTSP URL using Video LAN. If you do not have a VLC media player, download it for free at http://www.videolan.org/. Once installed go to **Start** > **All Programs** > **VideoLAN** > **VLC media player**. In the VLC media player **Media** menu, select **Open Network Stream**. Type the RTSP URL and click **Play**. Verify a connection. If there is no connection here, check the camera.<br>ii. Ping the IP address to verify connectivity. Go to **Start** > **All Programs** > **Run**. In the Run window type **cmd**. In the command prompt window, type ping <camera IP address>, and wait for a response. If no connection, the camera may be off.<br>If the camera is not listed and you are unsure of your camera's RTSP URL, check with the camera's manufacturer. |
| **Video Capture LRP URL** | **Advanced mode only.**<br>Check the checkbox to enable the Video Capture LRP URL. From the drop-down list, choose **rtsp://**.The RTSP URL allows for capturing low resolution video feeds.<br>• In the first text box, type the IP address or host name for the selected camera. The second text box populates automatically when a camera manufacturer and model are selected. You can also enter the entire URL manually.<br>• Click the **Test** button to test the RTSP URL. If the test is successful a Live View window appears. A successful connection should take no more than 10 seconds. If the test fails see the **Video Capture URL** element above for troubleshooting ideas.<br>If the camera is not listed and you are unsure of your camera's RTSP URL, check with the camera's manufacturer. |
| **Thumbnail URL** | **Advanced mode only.**<br>Check the checkbox to enable the Thumbnail URL. From the drop-down list, choose either **http://** or **https://**. The HTTP or HTTPS URL allows for producing images.<br>• In the first text box, type the IP address or host name for the selected camera. The second text box populates automatically when a camera manufacturer and model are selected. You can also enter the entire URL manually. |

© 2015

| Element | Description |
|---|---|
| | Thumbnail URL capabilities are not available with all camera manufacturers and models.<br><br>• Click the **Test** button to test the HTTP or HTTPS URL. If the test is successful a Live View window appears. A successful connection should take no more than 10 seconds. If the test fails see the **Video Capture URL** element above for troubleshooting ideas.<br><br>If the camera is not listed and you are unsure of your camera's RTSP URL, check with the camera's manufacturer. |
| **Live View URL** | **Advanced mode only**.<br><br>By default, the Live View URL is enabled and there will be a check in the checkbox. From the drop-down list, choose **rtsp://**. The RTSP URL allows a live view from your camera.<br><br>• In the first text box, type the IP address or host name for the selected camera. The second text box populates automatically when a camera manufacturer and model are selected. You can also enter the entire URL manually.<br><br>• Click the **Test** button to test the RTSP URL. If the test is successful a Live View window appears. A successful connection should take no more than 10 seconds. If the test fails see the **Video Capture URL** element above for troubleshooting ideas.<br><br>If the camera is not listed and you are unsure of your camera's RTSP URL, check with the camera's manufacturer. |
| **Management URL** | **Advanced mode only**.<br><br>Enables camera management from a Web browser when this type of functionality is supported by the camera. From the drop-down list, choose either **http://** or **https://**.<br><br>• With this checkbox selected, the boxes to the right are for the HTTP or HTTPS URL of the camera that enables you to manage your camera. This is an HTTP or HTTPS address provided by the manufacturer.<br><br>• Click the **Test** button to test the URL. If the test fails, ensure you have entered the correct URL and that your camera and camera manufacturer support online camera management. |

© 2015

| Element | Description |
|---|---|
| **User Name** | Type a User Name if the camera requires a user name and password to be accessed. This box works in conjunction with Password. |
| **Password** | Type a Password if the camera requires a user name and password to be accessed. This box works in conjunction with User Name. |
| **Alternative Frame Size** | **Advanced mode only**.<br>The width and height, in pixels, of video images. Use to define a frame size that is different from the camera's default. The first box is for width and the second is for height. |
| **Enable stream over TCP** | **Advanced mode only**.<br>Causes the RTSP capture to stream data over a TCP connection rather than over a default HTTP connection. |
| **Recording Computer** | The computer that captures a video feed from your camera. |
| **Access Permissions** | **Advanced mode only.**<br>Ability to add, change, or delete rights for a camera. Access permissions determine who has access to cameras and the access level. When working in **Standard** mode, the default permissions include "everyone" and "Recorded and Live Video and PTZ".<br>Double-click an existing security entry to change an entry, click the **Add** button to insert a new entry, click the **Delete** button to remove an entry, or click the **Up** or **Down** arrow buttons to change the order the entries are listed in the **Access Permissions** group box. See the Add New Security Entry section below. |
| **Active** | **Advanced mode only**.<br>Determine whether the camera is active or inactive. To capture video and view live feeds, this checkbox must be selected. If it is not selected, then any policy that uses this camera will not run. |

4. When you are finished selecting options and entering values in the Add New Camera window, click **OK**.

5. From the Camera Configurations toolbar, click the **Save** button to save the new camera configuration and add the camera to the Information Repository.

© 2015

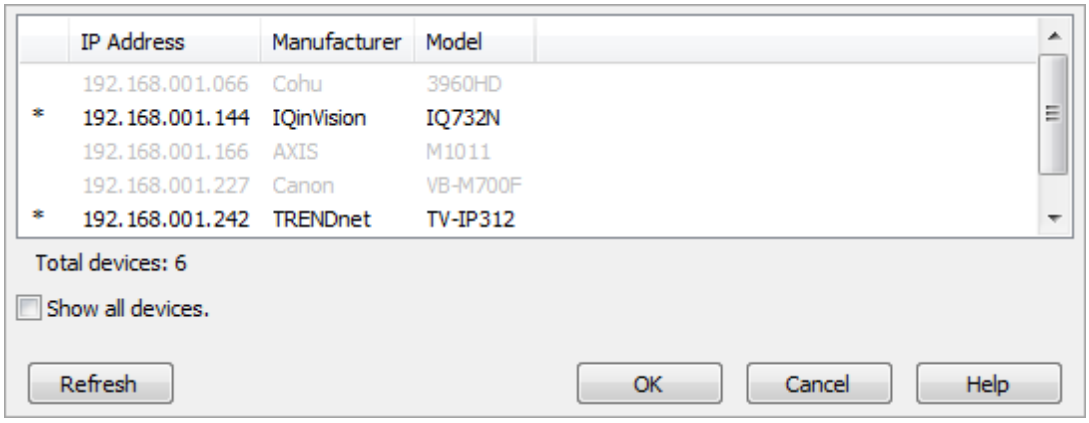
6. Repeat this process for each camera to add.

Phoenix RSM automatically configures camera settings and preserves motion detection metadata along with captured video when adding a RTSP-enabled IP camera. This data is then used by the Surveillance Video Manager (SVM) application to create histograms of detected motion. For more information see Motion Detection.

© 2015

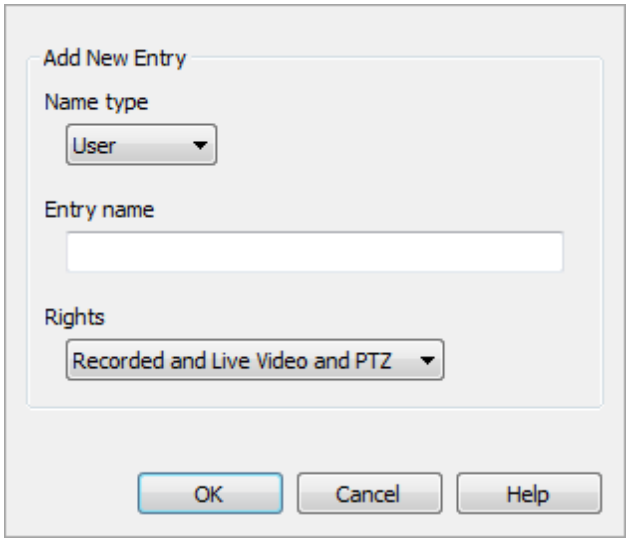
## Search Results window

From the Add New Camera window, click the **Find Cameras** button in order for the Search Results window to appear which will show a list of cameras found on the network. The camera list is pulled from a pre-populated list of manufacturers. If your camera is not on the list, select the **Show all devices** checkbox for any additional cameras on the network and other devices to display. If your camera still does not display, add it manually. In the Search Results window, cameras in use appear grayed-out and available cameras for configuration have an asterisk (*) in the first column. Select a camera and click **OK**, or double-click the camera item for the camera information to configure.




## Add New Security Entry

From the Add New Camera window, click the **Add New Security Entry** button under the **Access Permissions** group box. Use this window to insert a new access permissions entry. These permissions determine who has access to cameras and the access level.




**Name type** - Determine who the new security setting for a camera is applied to, or the type of rights; select between User, Group, Domain, and Everyone.

© 2015

**Entry name** - Type a name to appear under the **Access Permissions** group box.

**Rights** - Select the rights granted for the new user, group, domain, or everyone.

The rights are as follows:

- **Recorded and Live Video and PTZ** - Can view recorded and live video from selected camera and have PTZ control
- **Live Video and PTZ** - Can view live video and have PTZ control
- **Live Video** - Can view live video
- **Recorded and Live Video** - Can view recorded and live video from selected camera
- **Recorded Video** - Only view recorded video from the selected camera
- **None** - No access to the camera

If "recorded" is not included in user rights, you can still record using Live Viewer, but you will not be able to search for recorded video when using SVM.

## Add VMS Camera

To capture video into your Information Repository from your video management system (VMS), you need to create recording policies for cameras managed by those systems. Phoenix RSM tracks them and they are listed on the Camera Policies **Camera** tab for all computers on the network in the Information Repository.

Video capture from VMS may not be available, depending on your hardware device and your product license.

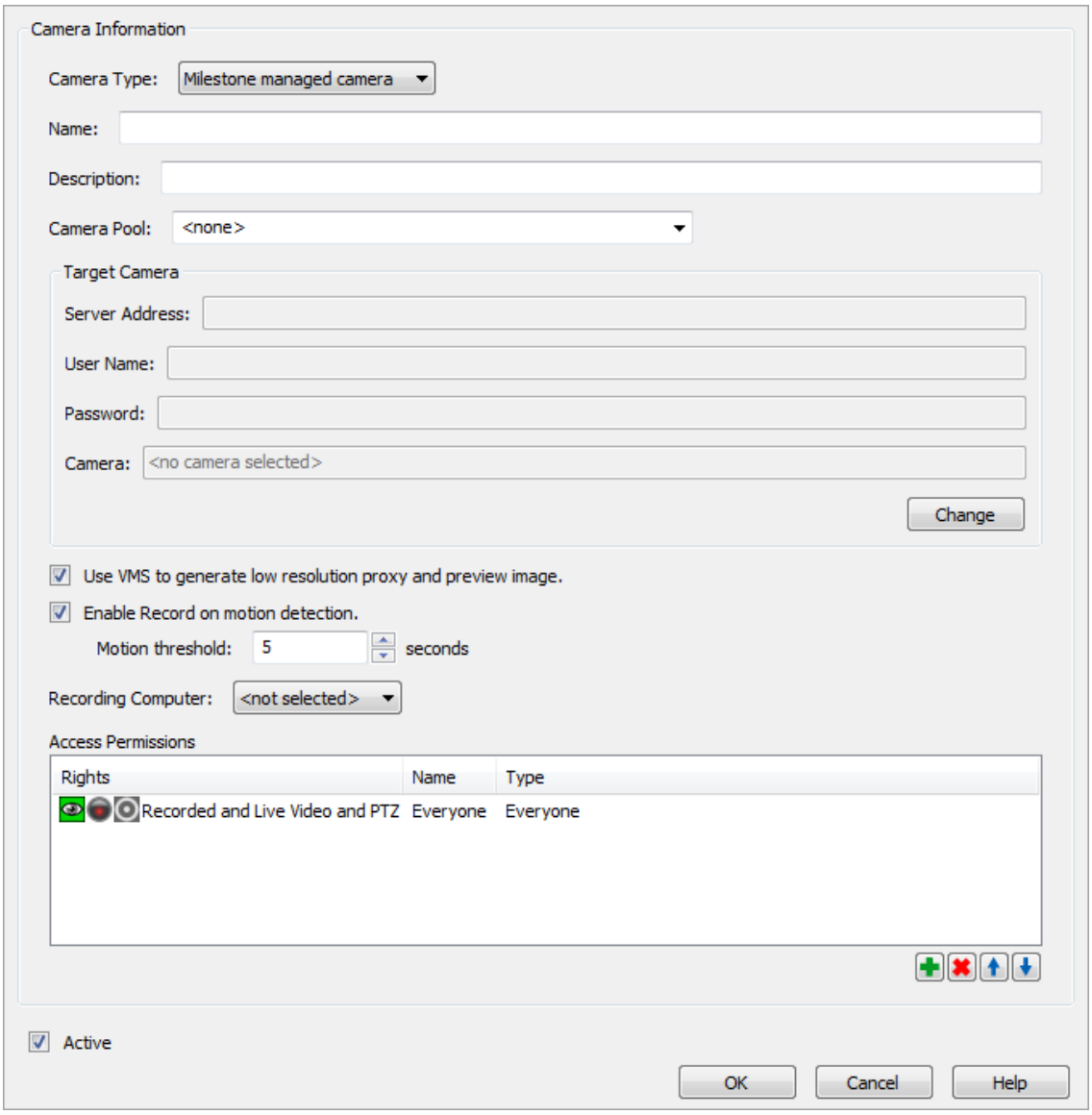
The supported VMS-managed solutions are Milestone XProtect, OnSSI, and exacqVision.

### To configure a Milestone, OnSSI, or Exacq managed camera:

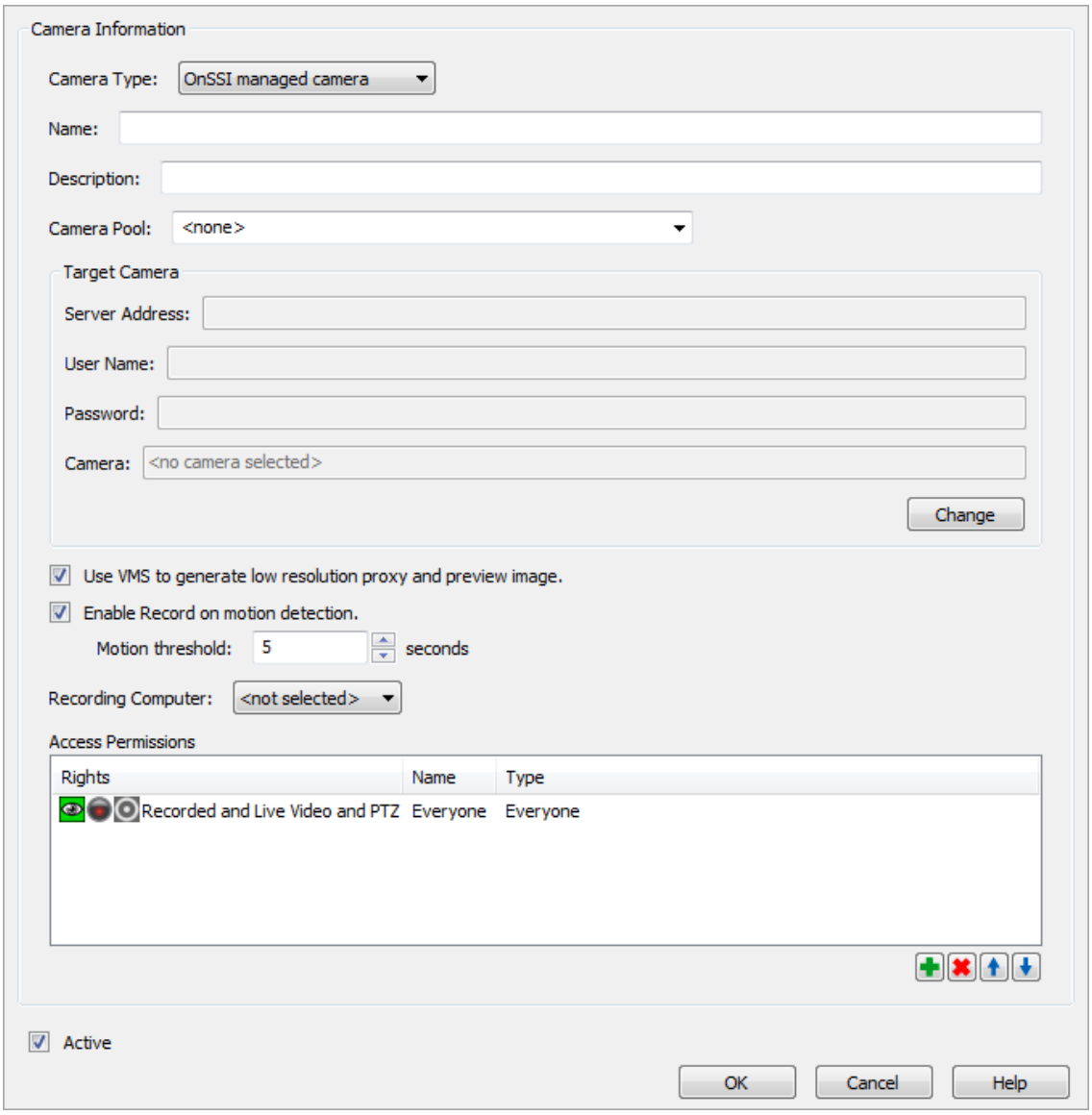
You must be in **Advanced Mode** to add a VMS camera.

1. From the Camera Policies **View** menu, select **Enable Advanced Mode**.
2. From the Camera Policies toolbar, click the **Cameras** button. The Camera Configuration window appears.
3. From the Camera Configuration window, click the **Add** button. The Add New Camera window appears. Fill in the necessary areas by using the table below.

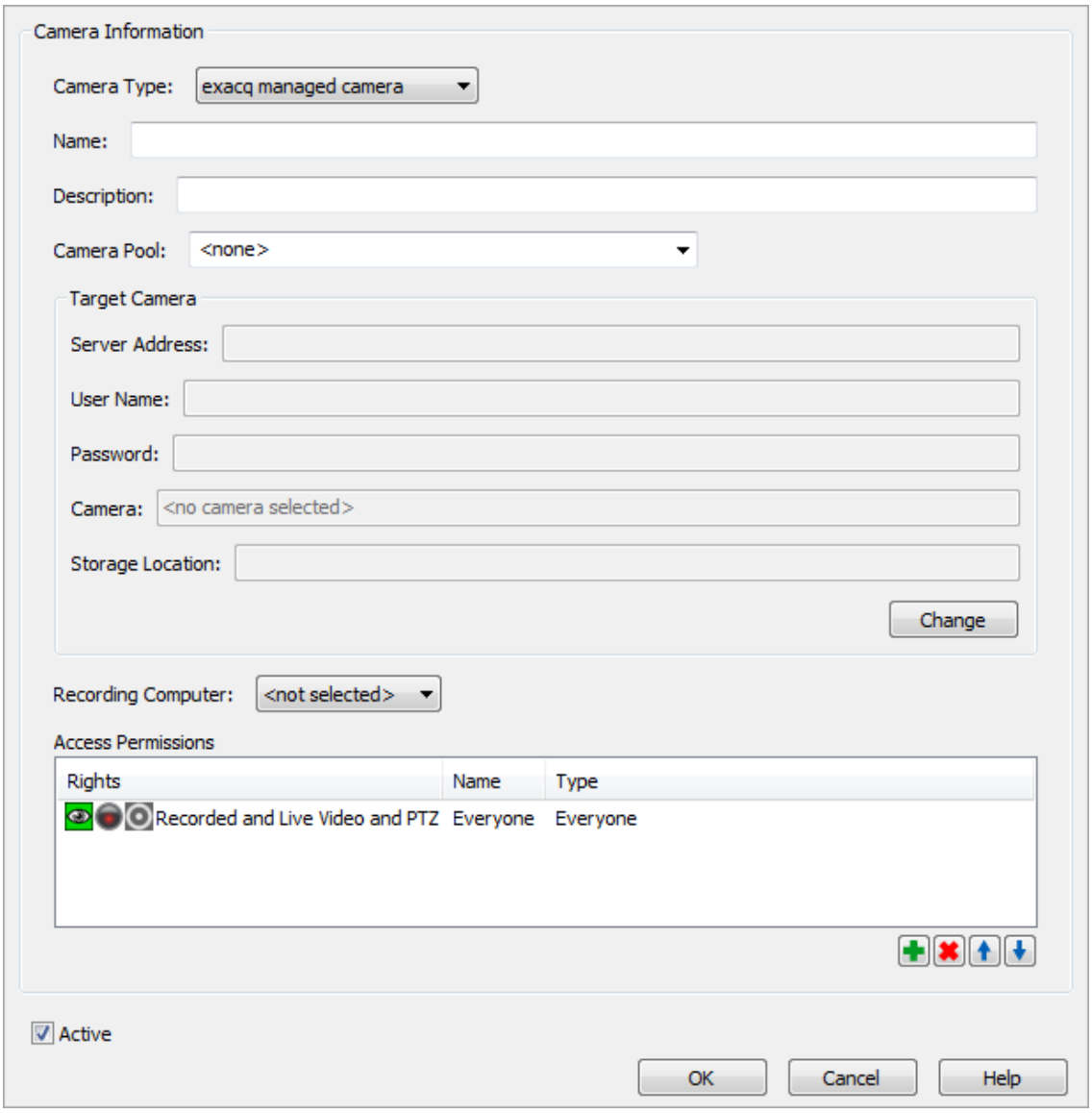
© 2015




OnSSI managed camera image:




exacq managed camera image:




| Element | Description |
|---|---|
| **Camera Type** | **Advanced mode only**.<br><br>The camera types can be an IP camera or a VMS-managed type of either Milestone managed camera, OnSSI managed camera, or exacq managed camera.<br><br>If your camera is not managed by a Milestone, OnSSI, or exacqVision video management system, see Manually Add IP Camera. |
| **Name** | Type a name used for menus and the configuration file, this is the name of the camera. |

© 2015

| Element | Description |
|---|---|
| | The name entered is for identification purposes only. It is best to use a naming convention and a descriptive name. |
| **Description** | Text used for defining the camera in menus and the configuration file. This is a description of the camera. |
| **Camera Pool** | **Advanced mode only**.<br><br>For the camera pool, define a virtual grouping of cameras to search video from specified cameras. For example, suppose you have a camera pool called "Doors". It is comprised of all the cameras that watch over the doors of your business. When you need to see who's come or gone, select the "Doors" camera pool as a search criteria, and only video captured from this camera pool are included. There is no limit to the number of camera pools your Phoenix RSM solution may have. |
| **Server Address** | The host name or IP address of the image server where you want to extract video. See the Modify Target Camera section below. |
| **User Name** | The User Name if the camera requires a user name and password to be accessed. This box works in conjunction with Password. See the Modify Target Camera section below. |
| **Password** | The Password if the camera requires a user name and password to be accessed. This box works in conjunction with User Name. See the Modify Target Camera section below. |
| **Selected Camera** | The camera whose video you want to capture. Click the **Refresh** button to update the list of cameras associated with the server. Select a camera. See the Modify Target Camera section below. |
| **Storage Location** | **For Exacq only**<br><br>The pathname to the video storage area. Type the path or click **Browse** to navigate to the video storage area. See the Modify Target Camera section below. |

© 2015

| Element | Description |
|---|---|
| | By default, Target and Process Service runs as Local System and may not have read access to network shares. Because of this, be sure to configure the video storage area to allow remote read access to everyone or change Target and Process Service to run with an account that will have read access. |
| **Use VMS to generate low resolution proxy and preview image** | **For Milestone and OnSSI only**<br><br>Select the checkbox to use the VMS to generate low resolution proxy and preview images. Currently this option is only supported when the camera is configured for jpeg mode. Selecting this option may increase the workload of the VMS server. |
| **Enable Record on motion detection** | **For Milestone and OnSSI only**<br><br>Select the checkbox to enable record on motion detection. Specify the **Motion threshold**, the amount of time to wait for motion before adding blank frames.<br><br>**For Milestone only:** The server can be set up to delete older recorded frames from its recording database by specifying the recording retention time. Any frames that are older than the set recording retention time will be automatically deleted. It is important that the retention time is long enough to always have recorded frames with motion in the database or specify the maximum recording storage size instead. |
| **Recording Computer** | The computer that captures a video feed from your camera. |
| **Access Permissions** | **Advanced mode only**.<br><br>Ability to add, change, or delete rights for a camera. Access permissions determine who has access to cameras and the access level. When working in **Standard** mode, the default permissions include "everyone" and "Recorded and Live Video and PTZ".<br><br>Double-click an existing security entry to change an entry, click the **Add** button to insert a new entry, click the **Delete** button to remove an entry, or click the **Up** or **Down** arrow buttons to change the order the entries are listed in the **Access Permissions** group box. See the Add New Security Entry section below. |

© 2015

| Element | Description |
|---|---|
| **Active** | **Advanced mode only**.<br><br>Determine whether the camera is active or inactive. To capture video and view live feeds, this checkbox must be selected. If it is not selected, then any policy that uses this camera will not run. |

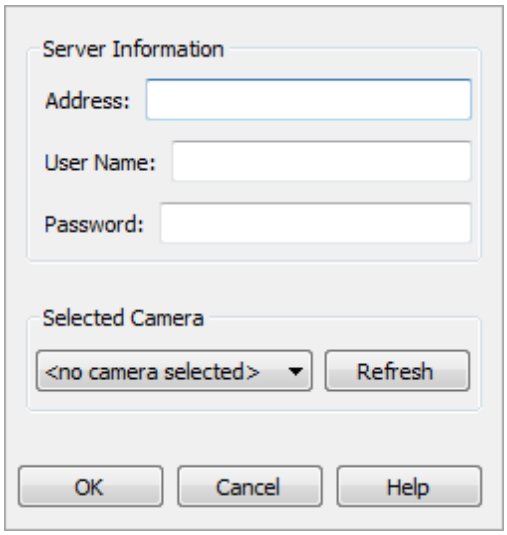
4. Click **OK** to close the Add New Camera window.

5. From the Camera Configuration window, click the **Save** button to save the new camera configuration and add it to your Information Repository. In the Camera Configuration window, Milestone, OnSSI, or exacq is evident in the Video Capture URL column, rather than RTSP.

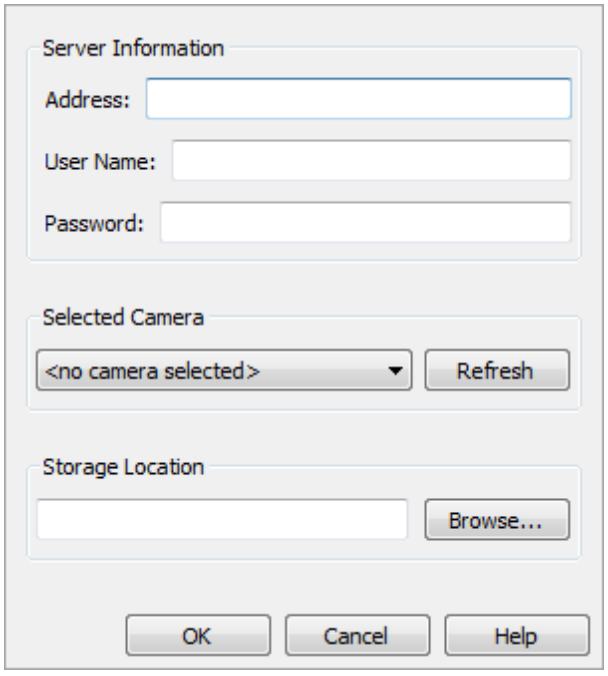
## Modify Target Camera window

From the Add New Camera window, click the **Change** button in the Target Camera area to open the Modify Target Camera window. Use this window to fill out the server information for the **Address**, **User Name**, and **Password**. In the **Selected Camera** section, click the **Refresh** button to update the list of cameras associated with the server. Select the camera whose video you want to capture.

**For Milestone and OnSSI:**



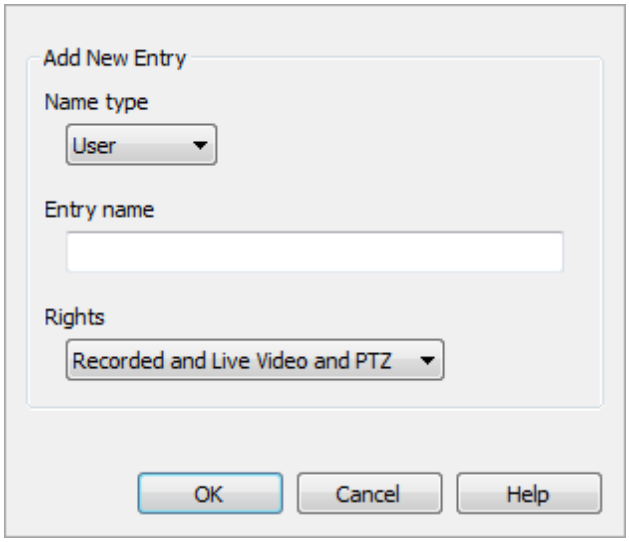

**For exacq only:** Fill in the **Storage Location** area with the pathname to the video storage area.




## Add New Security Entry

© 2015

From the Add New Camera window, click the **Add New Security Entry** button under the **Access Permissions** group box. Use this window to insert a new access permissions entry. These permissions determine who has access to cameras and the access level.




**Name type** - Determine who the new security setting for a camera is applied to, or the type of rights; select between User, Group, Domain, and Everyone.

**Entry name** - Type a name to appear under the **Access Permissions** group box.

**Rights** - Select the rights granted for the new user, group, domain, or everyone.

The rights are as follows:

- **Recorded and Live Video and PTZ** - Can view recorded and live video from selected camera and have PTZ control
- **Live Video and PTZ** - Can view live video and have PTZ control
- **Live Video** - Can view live video
- **Recorded and Live Video** - Can view recorded and live video from selected camera
- **Recorded Video** - Only view recorded video from the selected camera
- **None** - No access to the camera

If "recorded" is not included in user rights, you can still record using Live Viewer, but you will not be able to search for recorded video when using SVM.

## Motion Detection

Some RTSP-enabled IP cameras include or support motion detection. Depending on the camera type, Phoenix RSM supports motion detection information, automatically configures camera settings, and preserves motion metadata along with captured video. This data is then used by the Surveillance Video

© 2015

Manager (SVM) application to create histograms of detected motion.

The following describes how to configure cameras for motion detection. Supported camera types are AXIS and Panasonic.

## AXIS

When adding a RTSP-enabled AXIS IP camera using versions 2 or 3 of AXIS'S VAPIX API, the AXIS camera settings are configured and motion detection metadata is preserved with captured video. Default settings should be sufficient to meet most needs, but you can manually configure parameters that affect performance.

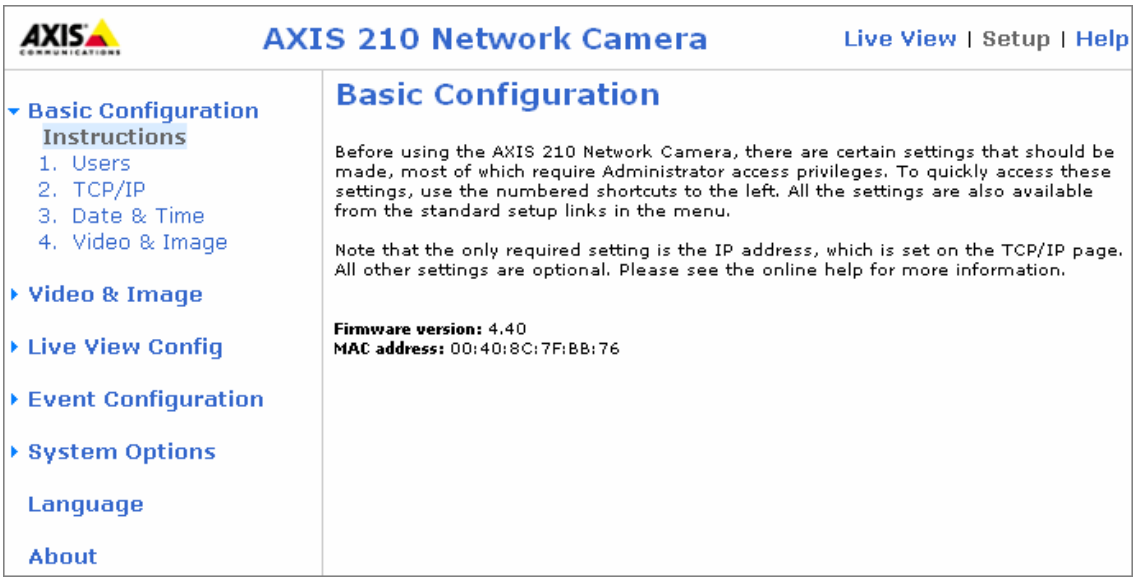
Be sure to see your AXIS camera's specifications to determine if your camera supports motion detection.

Except for **Image Compression** and **Motion Detection** settings, do not modify pre-set Phoenix RSM configuration settings for your AXIS camera, otherwise capturing motion detection data may not occur.

This configuration is intended for advanced users and documents only the AXIS network camera configuration. For more information about the AXIS network camera configuration web interface, see your specific AXIS camera documentation.

### AXIS camera motion detection configuration

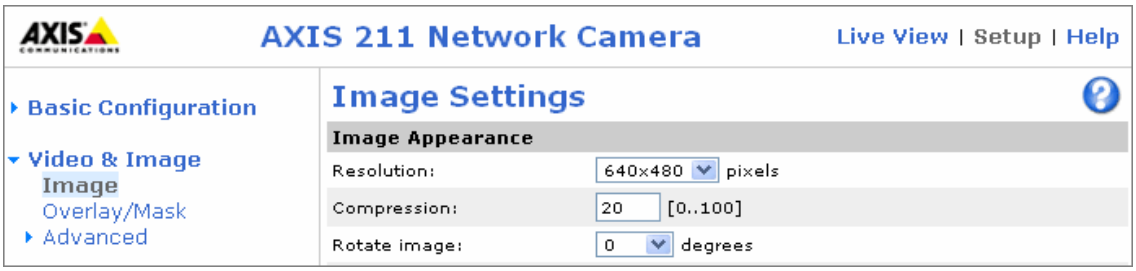
1. Open your AXIS camera management web interface.


AXIS 210 Network Camera
Live View | Setup | Help
Basic Configuration
Instructions
1. Users
2. TCP/IP
3. Date & Time
4. Video & Image
Video & Image
Live View Config
Event Configuration
System Options
Language
About
Basic Configuration
Before using the AXIS 210 Network Camera, there are certain settings that should be made, most of which require Administrator access privileges. To quickly access these settings, use the numbered shortcuts to the left. All the settings are also available from the standard setup links in the menu.
Note that the only required setting is the IP address, which is set on the TCP/IP page. All other settings are optional. Please see the online help for more information.
Firmware version: 4.40
MAC address: 00:40:8C:7F:BB:76

**Modify video image compression**

Phoenix RSM does not modify the default AXIS image compression parameter. To maximize performance and minimize loss of image quality, you may want to modify this value manually.

2. Select **Video & Image**. The Image Settings page appears.

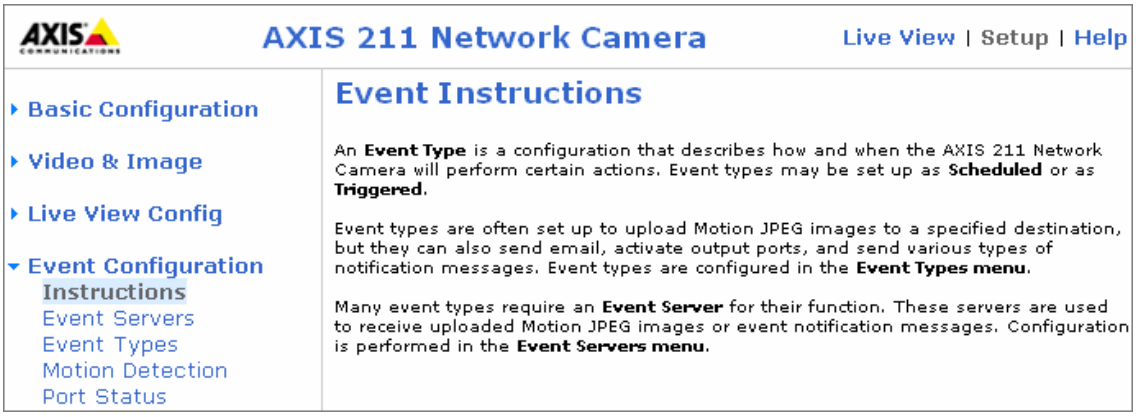



3. Set **Compression to 20**. This setting does reset if you disable and then enable the camera through your product. By selecting a setting less than 20, system performance may be impaired while motion is being recorded. By selecting a setting higher than 20, image quality may begin to degrade.

### Modify motion detection settings

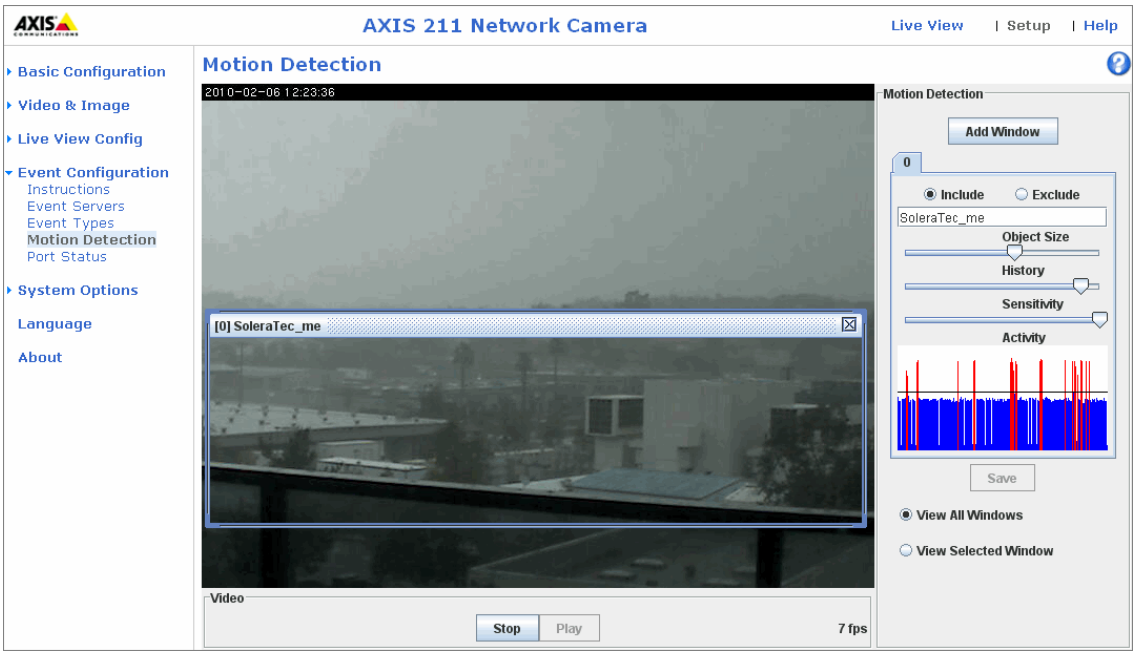
Along with video compression, you can change a camera's field of view that is covered by motion detection and motion detection sensitivity.

4. Select **Event Configuration**. The Instructions page appears.


AXIS 211 Network Camera
Live View | Setup | Help
Basic Configuration
Video & Image
Live View Config
Event Configuration
Instructions
Event Servers
Event Types
Motion Detection
Port Status
Event Instructions
An Event Type is a configuration that describes how and when the AXIS 211 Network Camera will perform certain actions. Event types may be set up as Scheduled or as Triggered.
Event types are often set up to upload Motion JPEG images to a specified destination, but they can also send email, activate output ports, and send various types of notification messages. Event types are configured in the Event Types menu.
Many event types require an Event Server for their function. These servers are used to receive uploaded Motion JPEG images or event notification messages. Configuration is performed in the Event Servers menu.

5. Select **Motion Detection**. The Motion Detection Page appears.

© 2015




Each camera supports one motion detection area. This is the part of the camera's field of view that is covered by motion detection. By default, the entire field of view is selected. You can change the covered area to suit your needs by dragging the borders of the motion detection area frame (titled SoleraTec_me above) and the entire frame itself so that it covers the area that you want monitored for motion.

6. Adjust the following parameters to suit your needs:

   - **Include** - By default, Include is selected and the motion detection area is titled SoleraTec_me. **Do not change these values**.
   - **Object Size** - Determine how large or small a moving object must be in order to trigger motion detection.
   - **History** - The number of frames against motion measured.
   - **Sensitivity** - How much change triggers a motion event.
   - **Activity** - Histogram of motion activity. The amount of activity displayed is determined by selected settings.

7. Click the **Save** button, when you are finished changing the motion detection settings.

## Supported Cameras

Your Phoenix RSM supports RTSP-enabled AXIS IP cameras using versions 2 or 3 of AXIS'S VAPIX API. For a complete listing of cameras, go to the AXIS online Product Interface guide: www.axis.com/techsup/cam_servers/dev/product_interface_guide.htm.

## Panasonic

© 2015

When adding a RTSP-enabled Panasonic camera that features motion alarms, the camera settings are configured and motion detection metadata is preserved with captured video. Default settings should be sufficient to meet most needs, but you can manually configure parameters that affect performance.

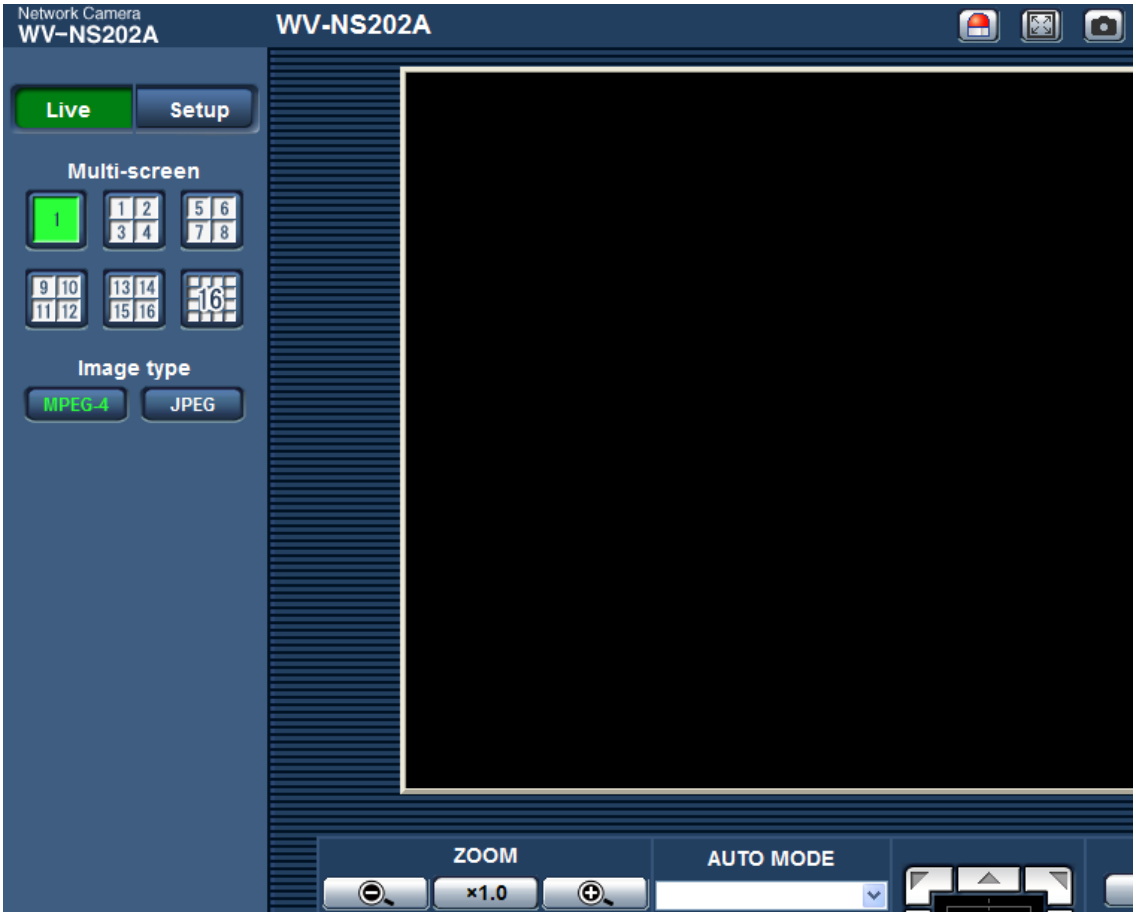
Be sure to see your Panasonic camera's specifications to determine if your camera features motion alarms.

This configuration is intended for advanced users and documents only the Panasonic network camera configuration. For more information about the Panasonic network camera configuration web interface, see your specific Panasonic camera documentation.

### Modify alarm and motion detection settings

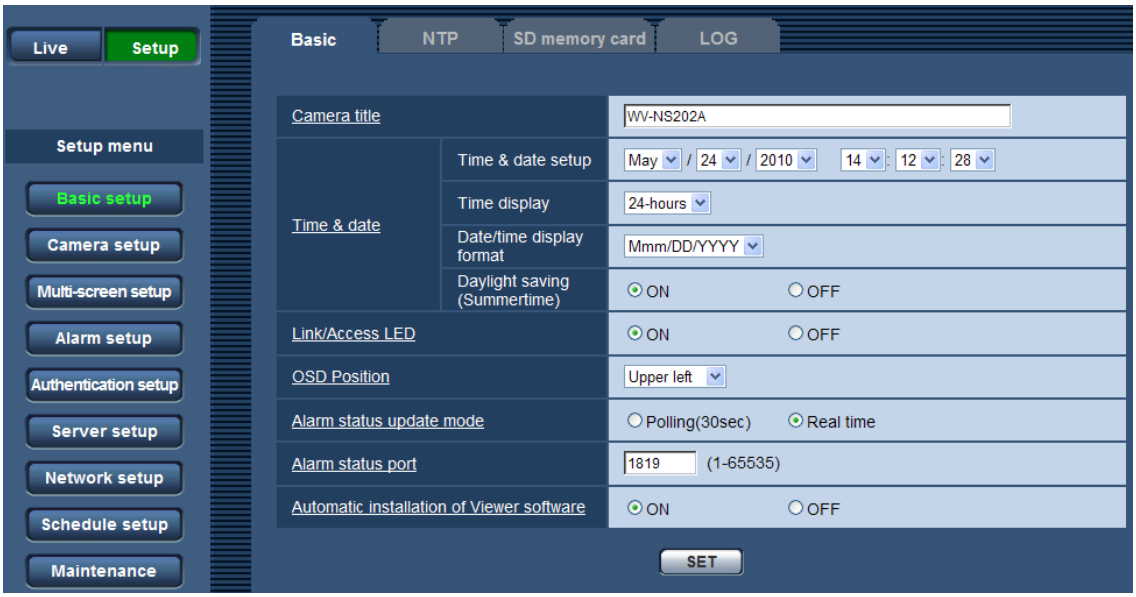
Use the Panasonic camera web interface to set customized motion alarms for up to four individual areas per camera. To capture motion metadata, set up motion alarms.

1. Open your Panasonic Network Camera management web interface.

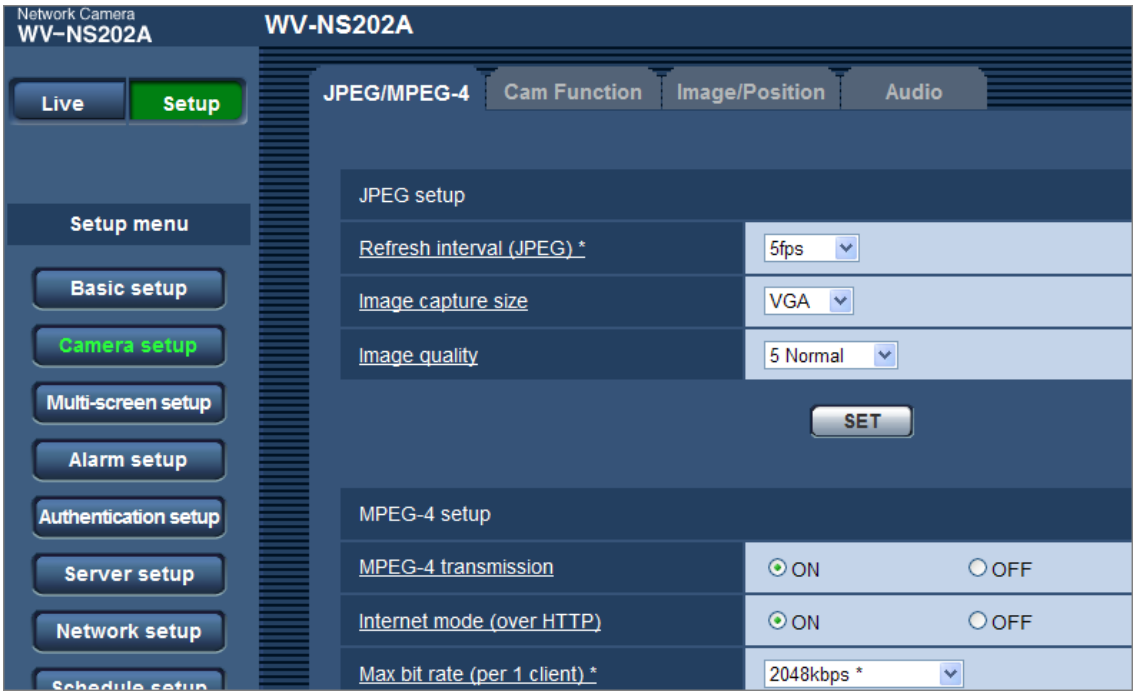



2. Select **Setup** for the Setup page to appear.

© 2015

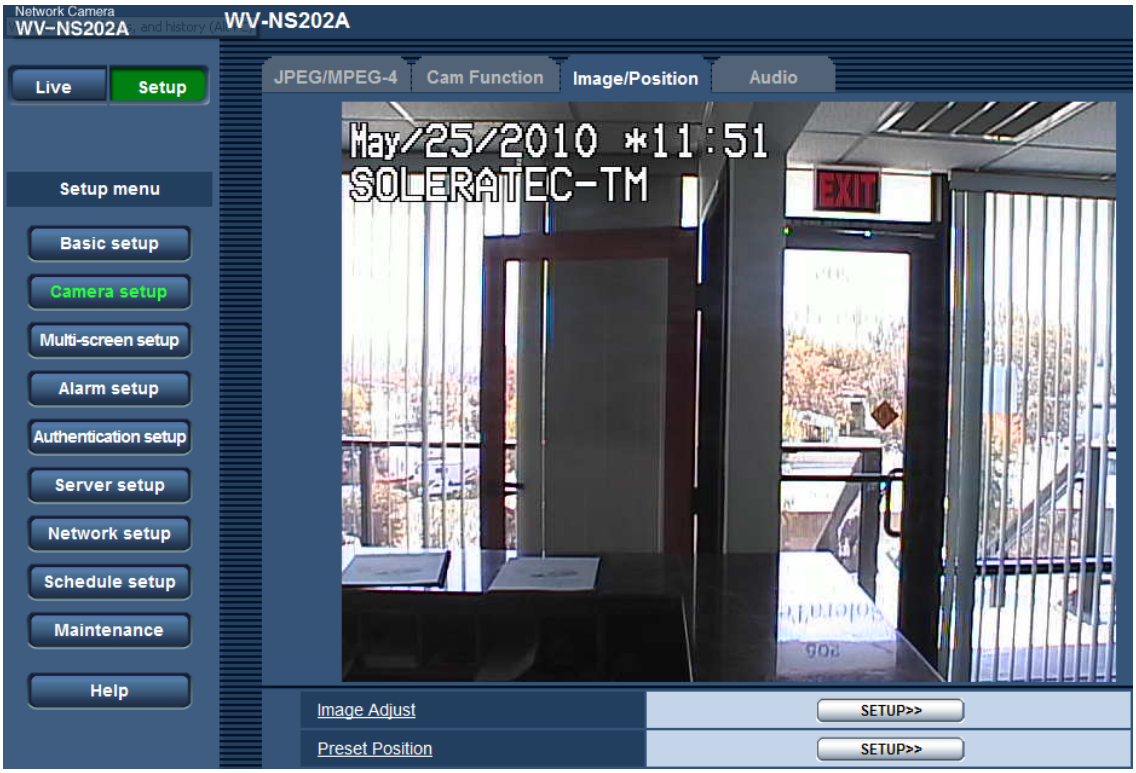



3. Select **Camera setup** for the Camera setup page to appear.




4. Select the **Image/Position** tab. Your camera's video feed appears with the date, time, and Preset ID listed at the top of the image. Ensure that **Preset ID** is set to SOLERATEC-TM:

© 2015




5. If the **Preset ID** is not set to SOLERATEC-TM, you need to set it. Beneath the video feed, find **Preset Position**, and then click **Setup**. The Position No page appears.

© 2015

6. In the **Preset No** drop-down list, select SOLERATEC-TM, and then click the **Set** button. In Position No 1, the **Preset ID** item should be set to **On**, and the **Preset ID (0 - 9,A - Z)** item should be populated with SOLERATEC-TM.

   If SOLERATEC-TM is not an option for **Preset No**, ensure that you have added your camera to the Information Repository correctly.

7. Select **Close** to exit the window and return to the Camera setup page, **Image/Position** tab. The **Preset ID** beneath the date and time should be SOLERATEC-TM.

8. Select **Alarm setup** for the Alarm setup page.

© 2015

9. Select the **VMD area** (Video Motion Detection) tab, and the video feed appears. The white square enclosing the video feed indicates the area that motion alarms can be set and motion detection metadata collected. Modify the following parameters:

   - **Status** - Turn motion alarms and motion metadata gathering on and off. When set to **On**, alarms are enabled and motion metadata is captured. When set to **Off**, alarms are disabled and no motion detection metadata is captured.

   - **Detection sensitivity** - Define the level of motion detected and recorded for the video feed area with a motion alarm. This area is the white square enclosing the video feed. Select from Super high to Low, with Super high being the most sensitive to motion. If you set **Preset position select** (below), the Detection sensitivity settings on this tab are ignored.

   - **Preset position select** - Define up to four discrete motion detection areas. If no areas are selected or are deactivated, then the system detects motion for the entire video feed area.

     Each camera supports up to four motion detection areas. This is the part of the camera's field of view where motion is monitored. By default, the entire field of view is selected. You can change covered areas by (1) deleting current areas, (2) creating new ones by dragging your cursor across the area you want covered, and (3) setting detection sensitivity. See the Preset Position Select section below for detailed directions for creating motion detection areas.

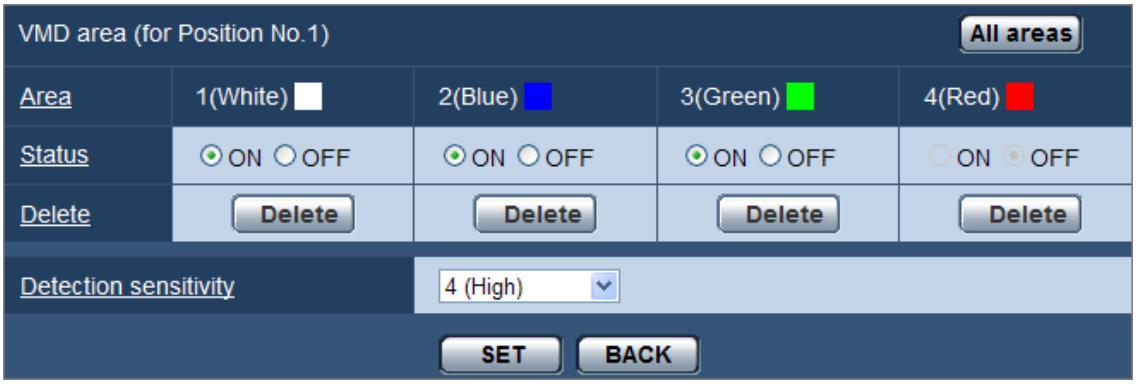
   - **Information addition** - Should be set to **Off**. It adds information, such as a timestamp, that is not used.

© 2015

10. Click **Set**, when you are finished changing your motion detection settings.

### Preset position select

1. Beneath the video feed on the **VMD area** tab find the **Video area** setting for Preset position section. Select Setup to the right of Preset position select. The VMD area page (for Position No.1) appears.




Each color-coded section represents one motion detection area. You can define up to four areas.

If you set Preset position select options, settings on the **VMD area** tab are ignored.

2. Change the covered areas to suit your needs by (1) deleting current areas and (2) creating new ones by dragging your cursor across the area you want covered.
3. Set the **Detection sensitivity** by using the options from the drop-down list.
4. Click **Set** to save and activate your settings.

### Supported Cameras

Your Phoenix RSM supports all RTSP-enabled Panasonic 202 series cameras.

# Live Viewer

Use SoleraTec's Phoenix RSM Live Viewer application to view live video feeds directly from RTSP-enabled IP cameras. View action as it is happening with the Live Viewer.

Before seeing live feeds, cameras must be configured in the Camera Policies application as part of your Information Repository. To view live feeds in the Live Viewer, the **Live View URL** checkbox must be selected and the IP address must be entered in the first field of the Video Capture or Live View URL when adding the camera configuration.

If this is done and you want to get started quickly, see View Camera Feeds

© 2015

To be able to view and record live video feeds, you must ensure that RTSP is enabled on your IP camera. See your camera's documentation for details on enabling RTSP.

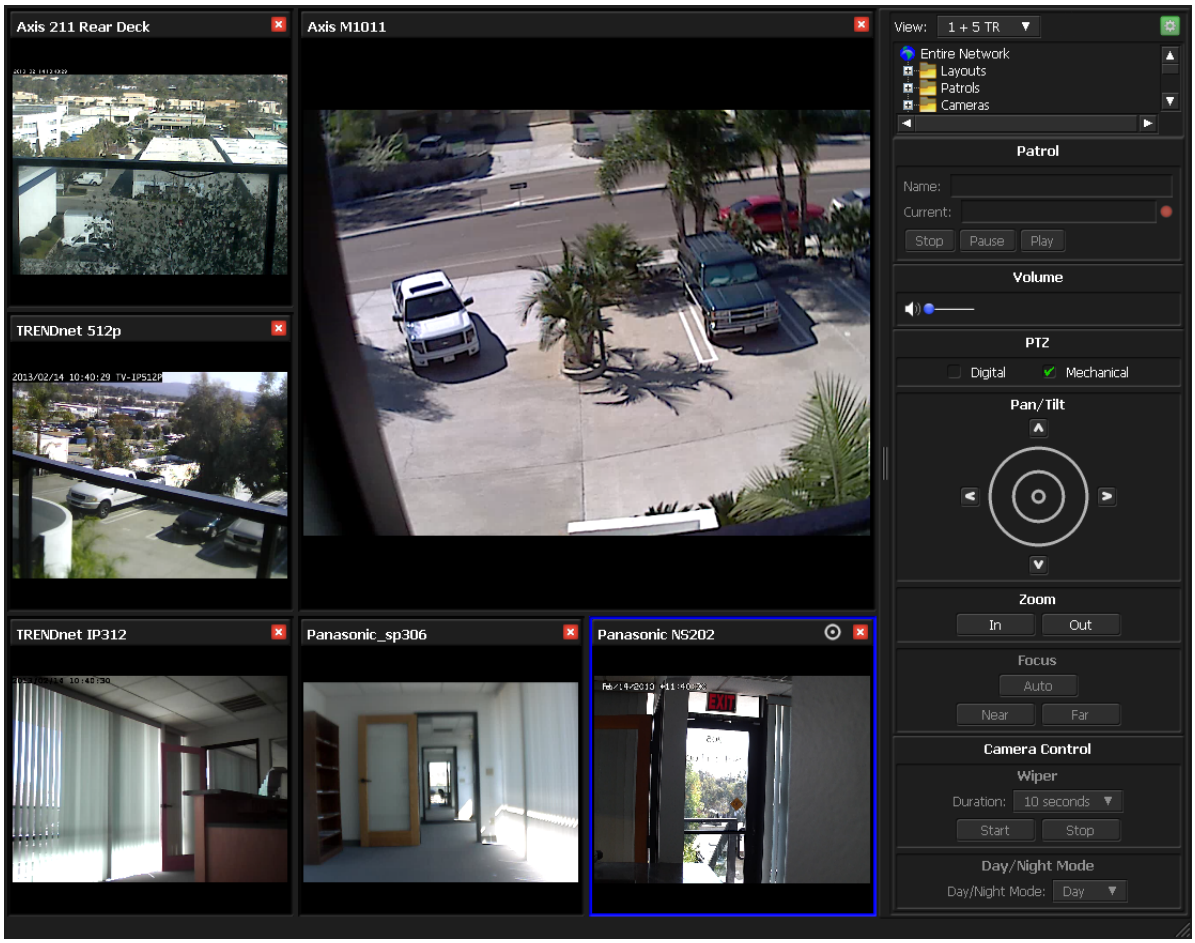
Most cameras can manage a single live feed while video streams are being captured. More than a single live feed on any given camera affects performance.

The Live Viewer window is divided into two main areas:

- **Control panel** - The right side of the Live Viewer includes several items of interest. From the **View** drop-down list, select a display layout for the Live Viewer window (the arrangement of camera ports). From the **Cameras** folder, select cameras which have the feeds you would like to view. From the **Patrols** folder you can create and manage patrols. There are also controls to access camera controls and the pan, tilt, zoom, and focus of cameras.

- **Camera ports** (or view frames) - On the left side of the window display are the live feeds from the cameras selected. By default, the Live Viewer is set to display feeds from four cameras, arranged in two rows of two across. Change that default layout by using the **View** drop-down list at the top of the right-hand control panel.

The screenshot below shows a layout with feeds from five cameras displayed. If you create a new layout, remember to save it so you can use it as your default layout.



In the Live Viewer, each camera view frame includes a **Title** bar. Right-click on the camera **Title** bar to display a shortcut menu with the following menu items (the **Enable advanced user mode** user preference must be selected to see the shortcut menu):

| Shortcut Menu Items | Description |
|---|---|
| **Select** | Highlight the camera view frame. Panel options are available, if applicable. |
| **Close** | Close the camera view (or click the **Close** button on the **Title** bar). |

Double-click the **Title** bar of the view frame for the camera to quickly change the default layout to a "port full screen" - taking the camera into and out of a 1x1 view. Double-click again to return to the original layout or press ESC.

## Live Viewer Menu Items

| Menu Items | Description |
|---|---|
| **File > Exit** | Close the application. |
| **View > Save Layout** | Save a modified camera layout with the same name. |
| **View > Save Layout As** | Create a new camera layout and save with new name. |
| **View > Rename Layout** | Designate a new name for the layout. |
| **View > Delete Layout** | Remove a layout from the Live Viewer. |
| **View > Create Patrol** | Select to open the Create Patrol window. |
| **View > Edit Patrol** | Use to change the name, layout sequence, or dwell time of the patrol. |
| **View > Rename Patrol** | Designate a new name for the patrol. |
| **View > Delete Patrol** | Remove a patrol from the Live Viewer. |
| **View > Full Screen** | Toggle full screen mode. To get out of full screen mode, press the ALT key, and then from the **View** menu deselect the **Full Screen** option. |

© 2015

| Menu Items | Description |
|---|---|
| **Tools > User Preferences** | Open the Live Viewer User Preferences window. |
| **Help > Current Page** | Open online help to the Live Viewer webpage. |
| **Help > Live Viewer Overview** | Open online help with focus on Live Viewer. |
| **Help > Contents** | Open the local version of online help. |
| **Help > Online Help** | Open the web-based version of online help. |
| **Help > Online Support** | Open the support webpage. |
| **Help > About Live Viewer** | Open the About Live Viewer window. |

When the main menu bar is hidden, click the from the Live Viewer Control panel to toggle between show and hide. If this **Show** menu bar button is not visible, try pressing the ALT key. Display of this item is managed in User Preferences.

For more information see Live Viewer Layout, View Camera Pool Feeds, and Camera Control: PTZ and Focus.

Advanced users can customize how a Live Viewer opens on startup through a command line prompt. For more information on arguments to use see Live Viewer Command Line.

## Control Panels

Control panels for the Live Viewer appear as a column on the right side of the Live Viewer. The entire panel can be minimized for maximum live viewing, or the panel can be maximized to manage your layouts, cameras, patrols, volume, and PTZ.

The **Title** bar of each control within the Control panel can be clicked to maximize or minimize viewing of the panel clicked.

To minimize the Control panel column, move the mouse pointer over the split line and click when the pointer becomes a hand. To maximize the Control panel column again, do the same action only this time the split line is near the window edge. Do the same action also, to maximize or minimize Title bar controls within the Control panel column.

### Camera Control Panel

This Control panel is only enabled if a view frame containing a camera that supports Wiper or Day/Night mode functions is selected.

© 2015

**Wiper** - Options for the camera wiper to clean. Duration options are: 10 seconds, 1 minute, 15 minutes, and 30 minutes, 1 hour, and 2 hours. Also select **Start** and **Stop** buttons. (Enabled only if camera has wiper functionality.)

**Day/Night Mode** - Options of Day, Night, and Auto. If Auto is selected the camera automatically adjusts to determine the correct mode. (This is enabled only if it is supported by Phoenix RSM for your camera, and if the camera has Day/Night Mode functionality.)

# View Camera Feeds

If the live view option is enabled from a camera during configuration, you can view a camera's live feed in the Phoenix RSM Live Viewer.

View live feeds from up to 16 cameras at a time.

### To view a live feed from a camera

1. Open the Live Viewer application.

   The Live Viewer window opens with the default layout. The **Title** bar for each camera port reads "Not in Use" as no cameras have been selected.

2. Expand the **Cameras** folder on the top right. The names of live view enabled cameras are displayed.

3. Select the camera feed to view and drag it into a camera view frame. The camera's live feed is displayed, and the camera name is displayed in the **Title** bar of the camera port.

4. To view the feed from an additional camera, repeat the step above.

To move one live feed to a different camera view frame, click the title bar and drag to the new view frame.

For more information see Live Viewer, View Camera Pool Feeds, and Live Viewer Layout.

# View Camera Pool Feeds

Camera pools are virtual groupings of cameras that you can define. For example, you might have a camera pool called "Doors" that includes all of the cameras that are videotaping the doors of your establishment.

It is often useful to see the live feeds from all of the cameras that belong to a certain pool. The Live Viewer lists camera pools as well as individual cameras to easily see the live feeds of cameras from a particular pool.

You will only see live feeds from cameras that are configured with the live view option enabled.

**How to create a camera pool:**

Camera pools are configured when creating a policy using Camera Policies.

© 2015

**To view live feeds from a camera pool:**

1. Open the Live Viewer application directly, or you can open it from the menu bar of the Surveillance Video Manager, select **Tools** > **Live Viewer**.

   The Live Viewer window opens with the default layout. The **Title** bar for each camera port reads "Not in Use" as no cameras have been selected yet.

2. Click the **Pools** folder on the top right. The names of the camera pools are displayed.

3. Select the pool to view and drag it into a camera view frame. Live views of the cameras contained in that camera pool are displayed in the viewer window. The camera name for each camera is displayed in the **Title** bar of its camera port.

For more information see Live Viewer Layout.

# Live Viewer Layout

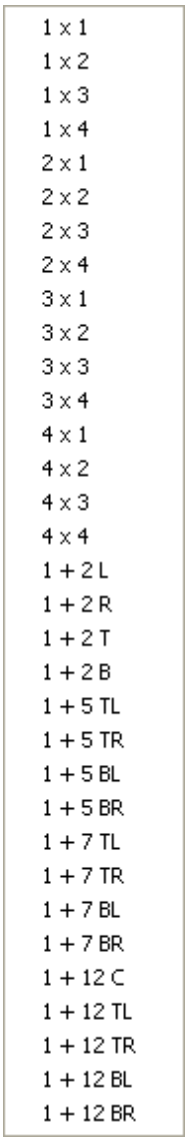
The first time opened, the Live Viewer is set to display four feeds from two cameras, arranged as "2x2" (two rows of two across).

You can change the default Live Viewer display by modifying, renaming, deleting, and then saving the new layout. The Live Viewer remembers the last layout opened and gives you the option to open it the next time you use Live Viewer.

### To change the Live Viewer display

1. Click the **View** drop-down list at the top of the right control panel.

© 2015




2. Select a view configuration.

   - For the views 1x1 through 4x4, the first number represents the number of live views across, in the row; the second number represents the number of rows, from top to bottom. You can view a maximum of 16 feeds (4x4) at a time.

   - In addition to the standard grid layouts, there are other layouts that feature one large view frame along with multiple smaller view frames (up to 12). The large view frame is positioned at the top left, top right, bottom left, bottom right, or center of the Live Viewer with the smaller view frames around it.

### To save a Live Viewer layout

1. Right-click the **Layouts** folder under the Entire Network area in the top right control panel, and select **Save Layout As**.

© 2015

2. In the Save As dialog box, type a name for the layout, and a description.
3. Click **OK**. The layout name is now listed under the Layouts folder in the Control Panel.

### To view a Live Viewer layout

1. Double-click the layout's name listed under the Layouts folder to view the selected layout.

### To rename a Live Viewer layout

1. Right-click the layout's name listed under the Layouts folder, and select **Rename Layout**.
2. Type a new name for the layout.

### To delete a Live Viewer layout

1. Right-click the layout's name listed under the Layouts folder, and select **Delete Layout**.

For more information see View Camera Feeds, View Camera Pool Feeds, and Live Viewer Patrols.

## Live Viewer Patrols

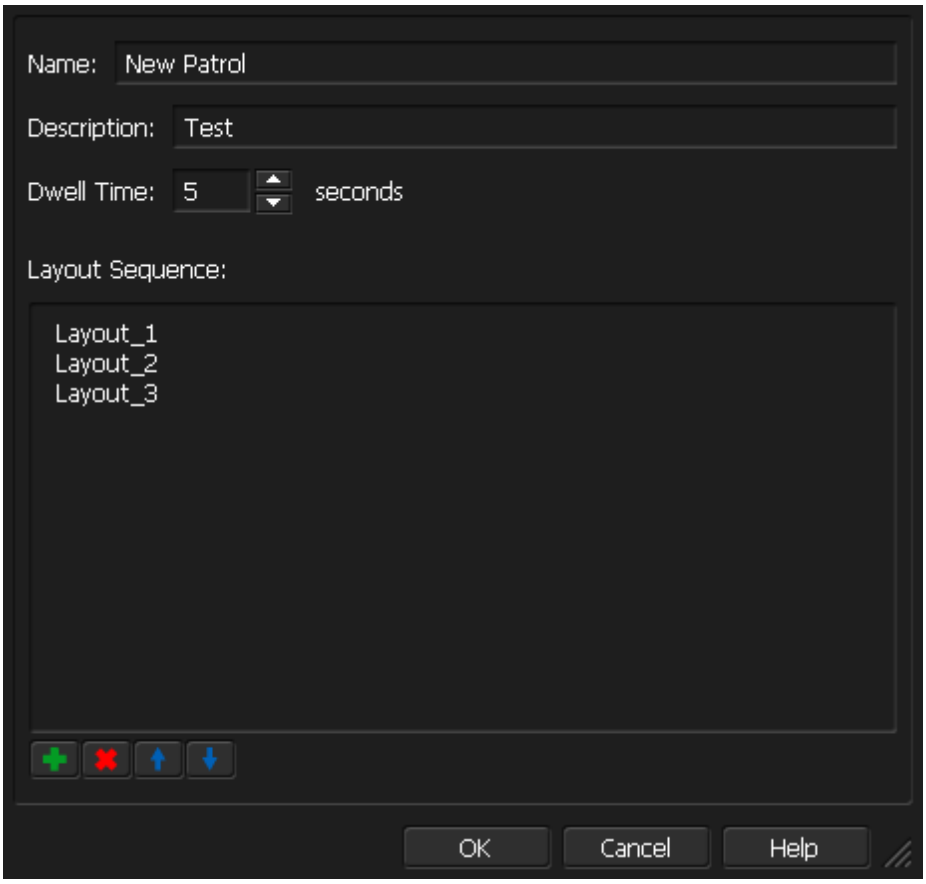
After you create Live View layouts, you can enhance your video surveillance ability by creating patrols. A patrol is a group of layouts, where each layout in a patrol is displayed in the Live Viewer for a set amount of time before the next layout is displayed.

You can create, edit, rename, or delete patrols from the Live Viewer **View** menu, or by right-clicking the **Patrols** folder under the Entire Network area in the top right portion of the control panel. Edit a patrol to change names, layout sequence, or dwell time.

### To create a patrol

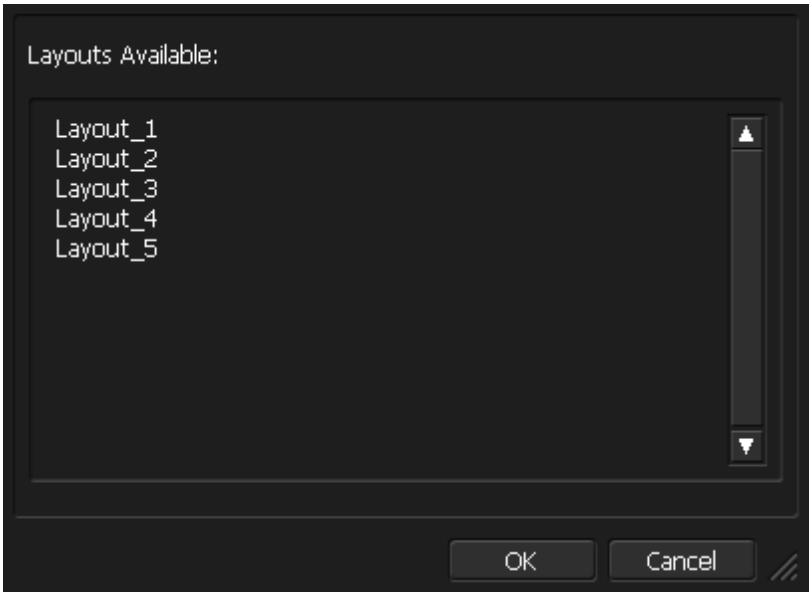
1. Create a few Live Viewer layouts.
2. From the **View** menu, select **Create Patrol**. The Create Patrol window appears.

© 2015




3. Type a patrol **Name**, a **Description** about the patrol, and select a **Dwell Time**. The dwell time is the amount of time that each layout is displayed in the viewer.

4. Select a Layout Sequence by clicking the **Add** button at the bottom of the Create Patrol window. The Select Layout window appears.




© 2015

5. Select a layout and click **OK**, or double-click the layout. The selected layout appears in the **Layout Sequence** box of the Create Patrol window. You can add more layouts, or remove a layout from the list, move a layout up or down in the list, by using the buttons at the bottom of the window.

6. From the **Patrols** folder, click the added patrol to activate the Patrol panel. The Patrol panel controls when to **Play**, **Pause**, or **Stop** the continuous loop of the patrol. The **Current** box displays which layout in the patrol is currently being displayed. Click the Patrol panel title bar to minimize or maximize the panel.

# Camera Control: PTZ and Focus

Phoenix RSM supports all IP configurable cameras, and most of the functionality of those cameras. Check to ensure that you have the correct access Rights to control PTZ. These Rights are controlled in Camera Policies.

If your camera supports mechanical PTZ, a white target symbol displays in the **Title** bar of the camera feed when it is displayed in a camera view frame of the Live Viewer. With all other cameras, you have the option of using digital PTZ (no white target symbol will be displayed). With the use of the Live Viewer, any camera can have PTZ functionality.

If you are running Windows, you can use any Windows-supported joystick to control the pan, tilt, and zoom of a camera. A joystick with X-Y axis capabilities is able to control the pan and tilt; a joystick with X-Y-Z axis capabilities is able to control the pan, tilt, and zoom. Joystick control can be used for mechanical and digital PTZ.

## Camera Control

Click the **Title** bar of the camera port for the camera. A blue border appears around the entire camera port to indicate the controls are active.

© 2015

### Digital or Mechanical PTZ

The top area of the PTZ control panel displays two radio buttons: **Digital** and **Mechanical**. The selection made here indicates the use of either digital or mechanical PTZ for controlling your camera.

1. If your camera has mechanical PTZ functionality, both options are available.

- Click the Digital radio button to use digital PTZ or click the Mechanical radio button to use mechanical PTZ.

Only one type of PTZ can be selected to use at a time.

2. If your camera does not have mechanical PTZ functionality, then Digital is automatically selected and the radio buttons are disabled.

© 2015

### To control a camera's pan and tilt

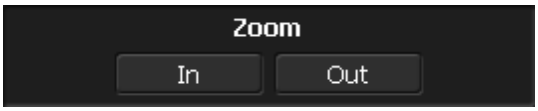
1. On the **Pan/Tilt** control panel at the right, click the left and right arrow buttons to pan the camera horizontally.

2. Click the up and down arrow buttons to tilt the camera vertically.

Alternatively, you can click and hold anywhere on the target graphic and then move your mouse to change the direction of the pan and tilt.

### To control a camera's zoom

1. On the **Zoom** control panel at the right, use the **In** button to zoom in on the center of the view. Use the **Out** button to zoom out from the center and include a wider angle of view.



A camera's zoom can also be controlled using the scroll wheel on a mouse. To do this, place the cursor over the target graphic in the **Pan/Tilt** area of the control panel. Move the scroll wheel forward (away from you) to zoom in and backward (towards you) to zoom out.

Because digital PTZ does not physically move the camera, you cannot view outside the camera's original view area. This means you can only use digital pan and tilt after zooming in on the live video feed.

### To control a camera's focus

1. On the **Focus** control panel at the right, use the **Auto** button to activate the camera's auto-focus feature. Use the **Near** button to focus on near objects in the foreground, and the **Far** button to focus on objects in the background.

© 2015

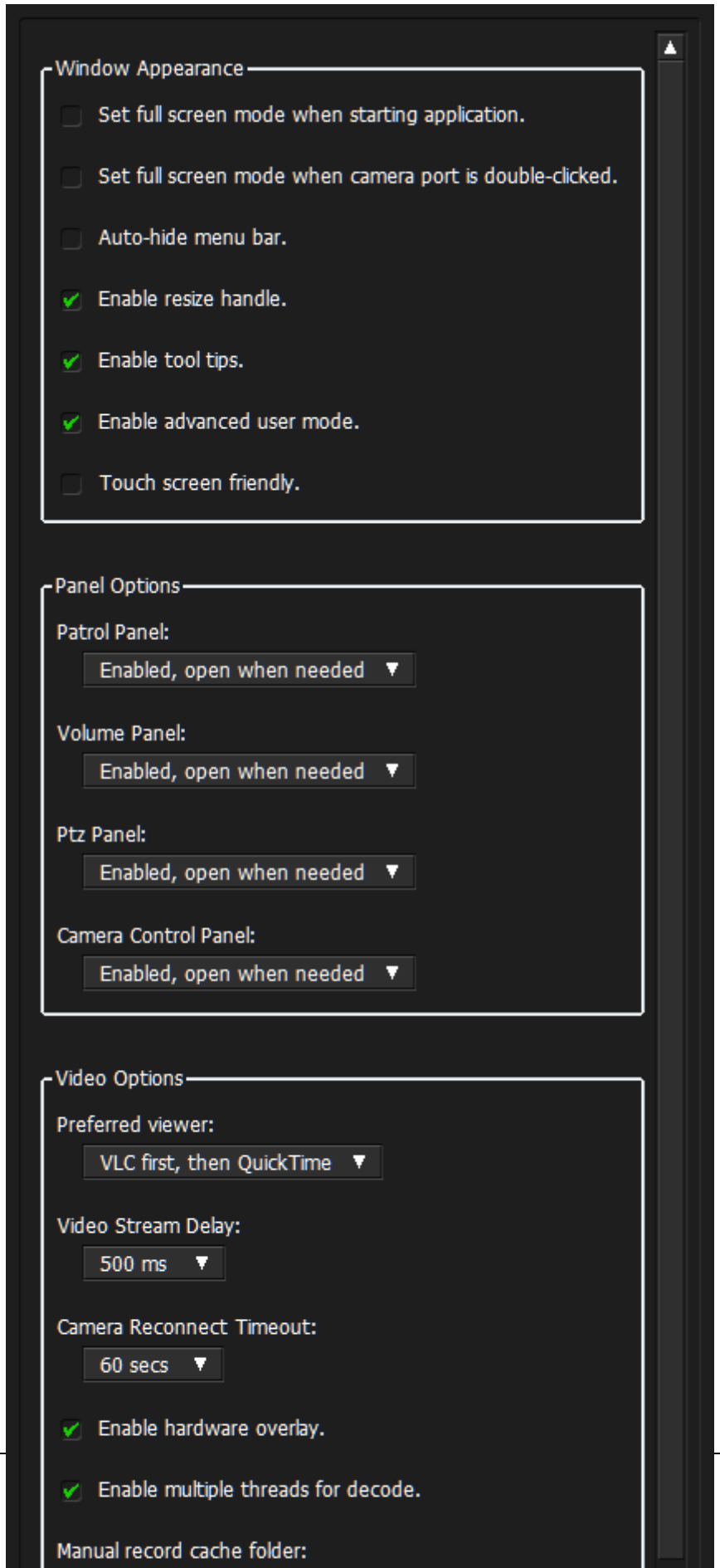
For more information see View Camera Feeds, View Camera Pool Feeds, and Live Viewer Layout.

## Live Viewer User Preferences

Use the Live Viewer User Preferences to define default settings for the Live Viewer window.

Access the Live Viewer User Preferences from the Live Viewer **Tools** menu, select **User Preferences**.

© 2015


Window Appearance
Set full screen mode when starting application.
Set full screen mode when camera port is double-clicked.
Auto-hide menu bar.
Enable resize handle.
Enable tool tips.
Enable advanced user mode.
Touch screen friendly.
Panel Options
Patrol Panel:
Enabled, open when needed
Volume Panel:
Enabled, open when needed
Ptz Panel:
Enabled, open when needed
Camera Control Panel:
Enabled, open when needed
Video Options
Preferred viewer:
VLC first, then QuickTime
Video Stream Delay:
500 ms
Camera Reconnect Timeout:
60 secs
Enable hardware overlay.
Enable multiple threads for decode.
Manual record cache folder:

© 2015

## Live Viewer User Preference Elements

| Element | Description |
|---|---|
| **Set full screen mode when starting application** | Select to start the Live Viewer application in **Full Screen** mode, where no **Title** bar or Windows **Start** bar appear. |
| **Set full screen mode when camera port is double-clicked** | When the camera port (or view frame) **Title** bar is double-clicked, it displays in **Full Screen** mode (with no **Title** bar or Windows **Start** bar). |
| **Auto-hide menu bar** | Select to hide the main menu bar.<br>• Press ALT to show the menu.<br>• Press ESC to hide it. |
| **Enable resize handle** | Display/hide the right hand bottom corner resize handle. |
| **Enable tool tips** | Tool tips display on screen if this is selected. De-select to turn tool tips off. |
| **Enable advanced user mode** | A check mark by this element allows the shortcut menu to display from the Live Viewer when you right-click the **Title** bar. The advanced mode shortcut menu features camera related options if the camera has the available functionality. |
| **Touch screen friendly** | Select the **Show** menu bar button to display or hide the main menu bar. Enabled if the Auto-hide menu bar and Touch screen friendly checkboxes are selected. If this button is not visible and you do not see the main menu bar, try pressing the ALT key. |
| **Patrol Panel** | Select from panel options:<br>**Enabled** - the panel is available.<br>**Disabled** - the panel is not displayed inside the side Control panel.<br>**Enabled, open when needed** - the panel is available and the functions are available when a view frame is selected. The panel is then maximized. |
| **Volume Panel** | Select from panel options:<br>**Enabled** - the panel is available.<br>**Disabled** - the panel is not displayed inside the side Control panel. |

© 2015

| Element | Description |
|---|---|
| | **Enabled, open when needed** - the panel is available and the functions are available when a view frame is selected. The panel is then maximized. |
| **PTZ Panel** | Select from panel options:<br>**Enabled** - the panel is available.<br>**Disabled** - the panel is not displayed inside the side Control panel.<br>**Enabled, open when needed** - the panel is available and the functions are available when a view frame is selected. The panel is then maximized. |
| **Camera Control Panel** | Select from panel options:<br>**Enabled** - the panel is available.<br>**Disabled** - the panel is not displayed inside the side Control panel.<br>**Enabled, open when needed** - the panel is available and the functions are available when a view frame is selected. The panel is then maximized. |
| **Preferred viewer** | Select the type of video viewer to drive the play back of videos. The orders to use the media players are: **QuickTime first, then VLC**, **QuickTime only**, **VLC first, then QuickTime**, or **VLC only**.<br> To play back videos in Phoenix RSM, you can use the supplied media player (VLC) or Apple QuickTime free or Pro on your computer. See Hardware and Software Requirements for the latest information. |
| **Video Stream Delay** | This selection determines how fast video feed streams to your camera view frame in Live Viewer. Changing the delay causes the video you are viewing to be delayed by that amount. The default value is 500 ms (milliseconds), but the options range from 0 ms to 3 seconds. A small delay value means the video can be viewed closer to real-time, but if the delay time is too small the video could freeze or hang. |

© 2015

| Element | Description |
|---|---|
| | Be sure to change the video stream delay setting before adding the camera to a view frame. If you change the preference after the camera has been added to the view frame, you will have to close it, change the setting again, and then re-add the camera to the view frame. If you close the Live Viewer application, your video stream delay preferences are saved, and ready for your next session.<br> If video freezes in low light conditions, set the video stream delay value to a larger value - at least 700ms or greater - especially on slow frame rate high definition cameras. |
| **Camera Reconnect Timeout** | Specifies the amount of time to try to reconnect to a camera if the connection is lost.<br>Choose an increment of time between 15 seconds and 30 minutes for the timeout.<br>If **Disabled** is selected, the Live Viewer will not attempt to reconnect to a camera. |
| **Enable hardware overlay** | Enable the hardware overlay capability of the video card. This enables the ability to render video directly.<br>If **Disabled**, remote desktop or shared desktop viewing may not work correctly for viewing live video streams. |
| **Enable multiple threads for decode** | Enable the use of multiple threads and multiple cores for decoding. This provides faster decoding of the video.<br>If decoding is not occurring properly, disabling this feature may fix the problem. |
| **Manual record cache folder** | Specify where to store Live Viewer recordings. Click the **Browse** button to navigate to the cache location using the Browse for Folder dialog box. |

For more information see Camera Control: PTZ and Focus and Live Viewer.

# Surveillance Video Manager

The Surveillance Video Manager (SVM) is SoleraTec's Phoenix RSM search application to find stored video on a Vault. It enables you to quickly and easily access, search, and review video from an entire library of forensic video assets.

© 2015

To use your video asset management solution effectively, capture your video with Camera Policies, search for and retrieve stored video using the Surveillance Video Manager, and then review video using the Media Viewer. Along with that functionality, you can view live video feeds with the Live Viewer. The Live Viewer supports many camera types, as it can connect and configure to any RTSP-enabled IP camera, and some motion-detection cameras. The Surveillance Video Manager can highlight the areas of the video with the most motion and action.

The search provisions in the Surveillance Video Manager are extensive, ultra-fast, and precise. As you search for video across your network, the Surveillance Video Manager uses a low resolution companion video (a fraction of the size of the original) as the primary video footage received. This low resolution companion file is always teamed with its original source video, regardless of where the video is stored (online, near-line, or offline). After searching for and retrieving video assets, you can export the video to other tools and locations. For more information see Introduction.

In order to have the low resolution companion video and thumbnail files available, be sure to enable them when setting up your recording policies. See Camera Policies, Processing tab.

The Surveillance Video Manager window features two main tabs at the top of the application to switch between the search or export functionality.

- **Search** - Comprised of a **Search Criteria** pane to find video files, a **Search Results** pane to select specific files from searched video and play in a Media Viewer, and an **Export Queue** pane to view a list of video to export.
- **Export** - Includes an **Export Job Configuration** pane and a **Job Status** pane to use when you are ready to export files found.

## Workflow - Surveillance Video Manager

In order to use the Surveillance Video Manager, video must be stored in a Vault and the Vault needs to be running. It is necessary to have set up a recording policy in Camera Policies to move video from a camera into a Vault. An administrator can find more information regarding these requirements at Add Vaults and Camera Policies.

The following describes working through the Surveillance Video Manager:

1. From your suite of product applications, open the Surveillance Video Manager application (SurveillanceVideoManager.exe). For further explanation of how to launch applications using different operating systems, see Getting Started.
2. The application default opens to the **Search** tab. Enter search criteria and click the **Search** button when done to begin the search. See SVM Search and Export.
3. When the search is complete, the results display in the Search Results pane.
4. Click a video thumbnail to open a recorded low resolution companion video in the Media Viewer.
5. Use the Media Viewer to review and play the video, and clip portions of the video to export. Click the **Export** button to send video clips to the Export Queue.

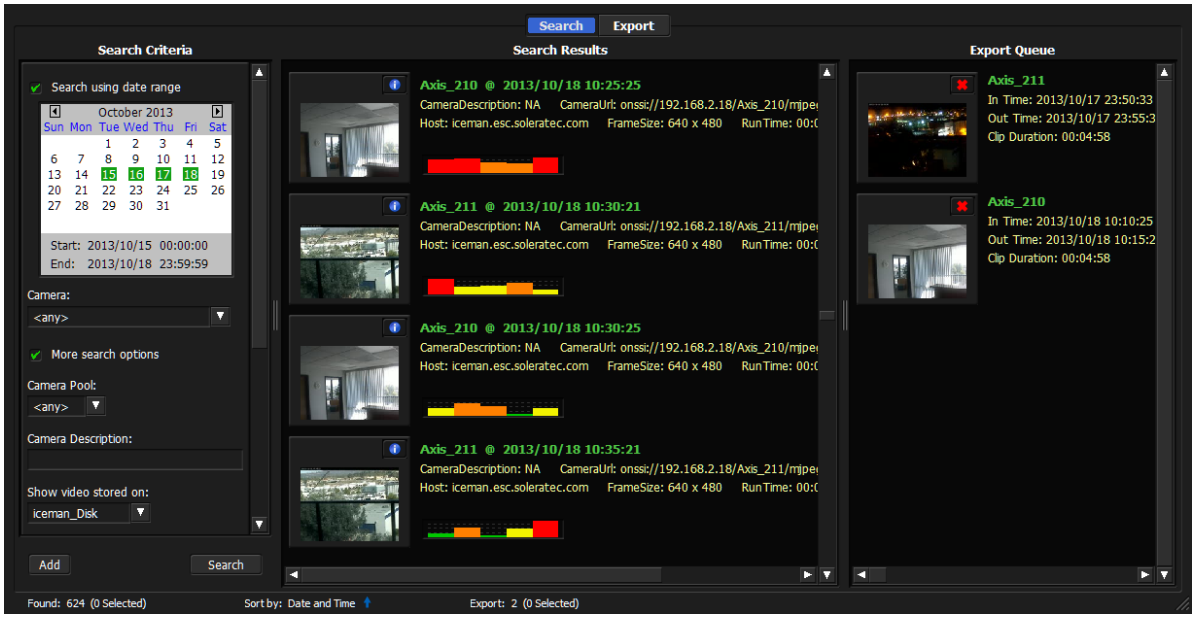
© 2015

6. Select the Surveillance Video Manager **Export** tab to set your Export Job Configuration options. This is where you determine what system to export to, where to save files, and other options. Click **Start Export**. Files in the Export Queue are exported all at once. See Export Surveillance Video.

For more information on how to search for, review, and export video files, see Search Surveillance Video.

# SVM Search and Export

## Search




Once you open SoleraTec's Surveillance Video Manager, the **Search** tab is in focus and ready to perform powerful searches on stored video files. As mentioned in the chapter overview, the Surveillance Video Manager's **Search** tab includes three panes to easily fulfill all your search and export needs:

- **Search Criteria** - Use to select and enter minimal or extensive search parameters to obtain relevant search results. Click the **Add** button to append more search parameters for a more focused search. Click the **Search** button to execute a search on the Information Repository.
- **Search Results** - Displays found videos based on Search Criteria. Right-click on a thumbnail to choose an action to perform. Double-click a thumbnail to view a low resolution proxy video in a Media Viewer. The Media Viewer offers the capability to select parts of video clips for export. At the bottom of this pane a total number of items found displays and a sort filter. Click a sort option to help locate your exact file.

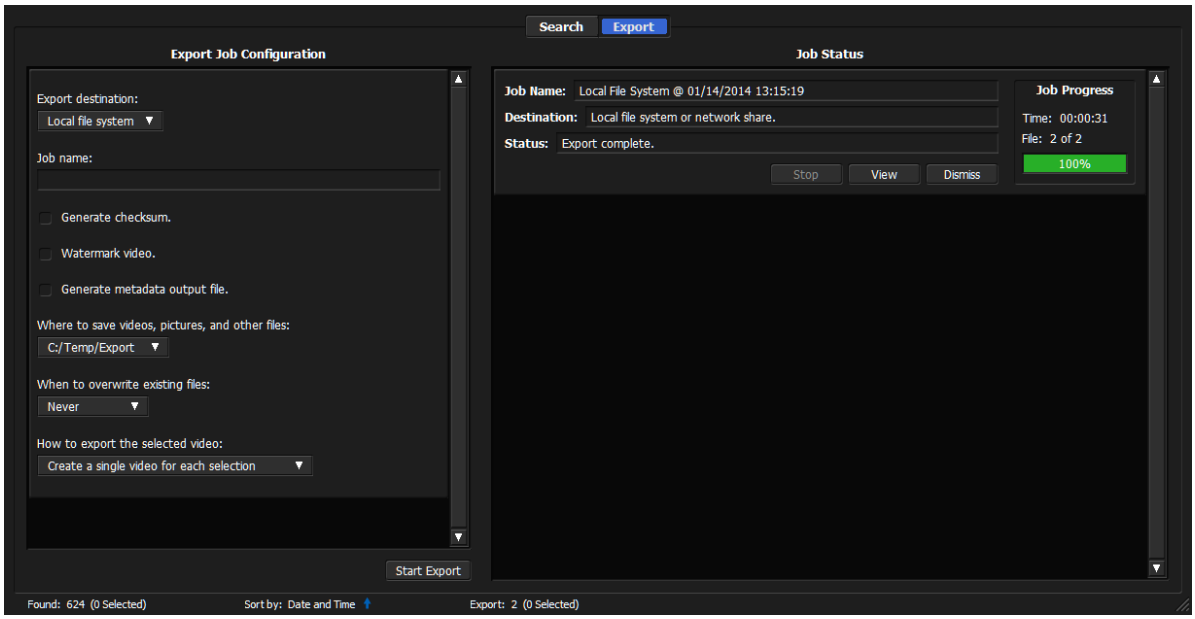
  To play videos in the Media Viewer, you can use the supplied media player (VLC) or Apple QuickTime version 7 or newer (free or Pro) needs to be installed on your computer. For viewing surveillance video, VLC works best.

- **Export Queue** - Displays videos selected for export. Right-click on a thumbnail in the Export Queue to choose an action to perform.

© 2015

Maximize the Search Results pane to allow maximum viewing area by minimizing the Search Criteria and Export Queue panes. To minimize either the Search Criteria or Export Queue pane, move the mouse pointer over the split line and click when the pointer becomes a hand. To maximize the panes again, do the same action only this time the split line is near the window edge.

## Export




The Surveillance Video Manager **Export** tab consists of two panes for exporting a job:

- **Export Configuration** - Select specific parameters for video to export. You can export video to a local file system, a Rimage system, or through FTP. Each type of export has its own configuration options. Select the **Start Export** button to begin exporting videos.
- **Job Status** - Displays results as videos are exported.

### Surveillance Video Manager Menu Items

| Menu Items | Description |
|---|---|
| **File > Export Queue** | Select an option from the drop-down list.<br>**Load from -** Load the Export Queue selections from a file.<br>**Save as -** Save the Export Queue selections to a file. |
| **File > Exit** | Close the application. |

© 2015

| Menu Items | Description |
|---|---|
| **View > List** | Select this option to display the search results as a list. Each video in the search results will be displayed as a preview image, filename, and other basic details about the video. |
| **View > Details** | Select this option to display the search results as a thumbnails with details. Each video in the search results will be displayed as a large thumbnail, a filename, and an in depth list of details about the video. |
| **View > Sort Results** | Choose how the search results should be sorted.<br>• The options to choose from are Camera and Date and Time.<br>• Your metadata fields are also available as Sort field options.<br> If sorting based on a metadata field, SVM will sort your results based only on the first 64 characters of the field you selected.<br>• From the **Sort order** drop-down list, choose either **Ascending** or **Descending**.<br>• Click **OK** to sort results. |
| **View > Status Bar** | A check mark by this menu item will display the status bar at the bottom of the Surveillance Video Manager window. It shows the number of files found, how the files are sorted, and how many files will be exported. |
| **Actions > Search Results** | Choose an action to perform on the videos and images in the Search Results pane.<br> This menu can also be accessed by right-clicking on a video in the Search Results pane.<br>• **Show Metadata** - Select to show and edit the metadata for the video.<br>• **Select All** - Select all of the videos in the Search Results.<br>• **Unselect All** - Unselect all of the videos in the Search Results.<br>• **Send to Export Queue** - Send the selected video to the Export Queue. |

© 2015

| Menu Items | Description |
|---|---|
| | • **Play -** Open the Media Viewer with the selected video queued up and ready to play. |
| **Actions > Export Queue** | Choose an action to perform on the videos and images in the Export Queue pane.<br> This menu can also be accessed by right-clicking on a video in the Export Queue pane.<br>• **Show Metadata** - Select to show and edit the metadata for the video.<br>• **Rename Export File** - Select to rename an export file or reset file to the original name.<br>• **Remove From Export Queue** - Remove the selected video from the Export Queue.<br>• **Select All** - Select all of the videos in the Export Queue.<br>• **Unselect All** - Unselect all of the videos in the Export Queue.<br>• **Play -** Open the Media Viewer with the selected video queued up and ready to play. |
| **Tools > User Preferences** | Open the Surveillance Video Manager User Preferences window. |
| **Help > Current Page** | Open online help to the Surveillance Video Manager webpage. |
| **Help > Surveillance Video Manager Overview** | Open online help with focus on Surveillance Video Manager. |
| **Help > Contents** | Open the local version of online help. |
| **Help > Online Help** | Open the web-based version of online help. |
| **Help > Online Support** | Open the support webpage. |
| **Help > About Surveillance Video Manager** | Open the About Surveillance Video Manager window. |

For more information see Search Surveillance Video and Export Surveillance Video.

© 2015

# Search Surveillance Video

The Surveillance Video Manager is designed to support your business with powerful search capabilities and review of surveillance video. With Phoenix RSM, all of your video assets are fully managed. The acts of finding, reviewing, and selecting video are the first steps to exporting your video. You can export entire videos or just clips of interest.

The following are instructions to give you a better idea on how to search for, review, and then select video for export using the Surveillance Video Manager tool:

1. Launch the Surveillance Video Manager.
2. The Surveillance Video Manager opens with the **Search** tab in focus. In the Search Criteria pane, begin your search for video by selecting a date range, camera type, or opt for more search options. Work your way through the search criteria by entering values for the search type.
    - More search options include: Camera Pool, Camera Description, Show video stored on, Show video captured by this computer, Show video stored on this media, and Show video stored in this storage pool.

## Search

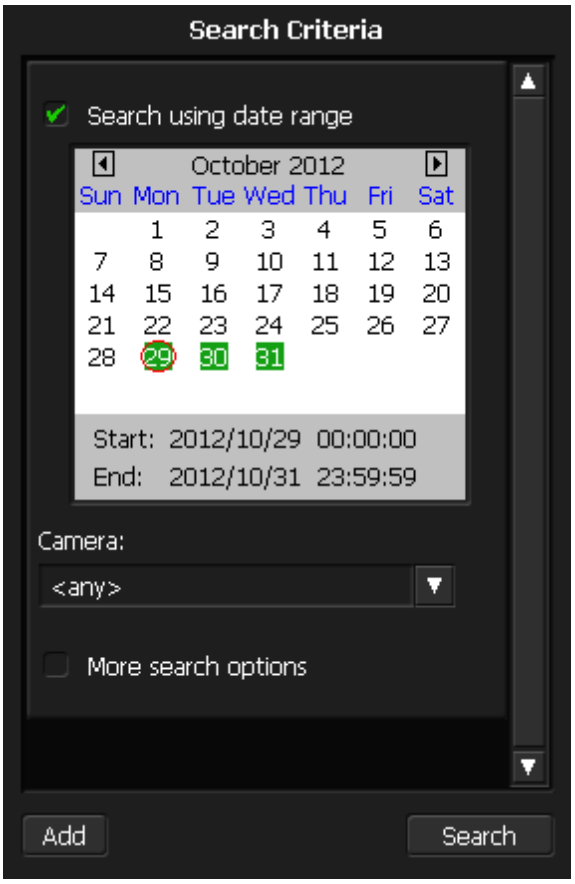
Carry out either broad or specific searches using this search tool. Define fewer search parameters for a broader set of results, or define more parameters for more relevant search results.

In order to get better search results for clips that have log entries associated with them, turn on **Search for preview images**, **Search for low resolution proxies**, and **Search for related files** in User Preferences.

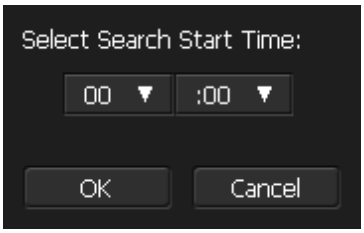
3. Search for video - To search for video captured on a particular date or between particular dates and times, select **Search using date range** (this activates calendar control).

When activated, the calendar control is interactive for you to select a start date, end date, and times to search. The top of the calendar control displays the months and dates, while the bottom features start and end times.

© 2015

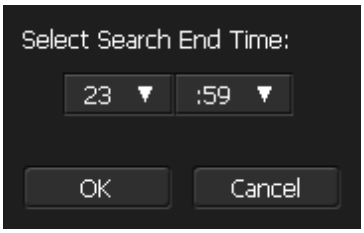



- Click on the calendar to select a search date range: Click the start date and from the shortcut menu that appears, select **Start Date**; click the end date and select **End Date**. (Start and end date can be the same.)
- Use the calendar to select a search time range within selected search dates. Click the start date and from the shortcut menu that appears, select **Start Time**.




- In the Start Time window, select a time and click **OK**.
- Click the end date and from the shortcut menu that appears, select **End Time**.

© 2015




- In the End Time window, select a time and click **OK**.

To search all stored video regardless of date and time, de-select the **Search using date range** checkbox.

4. Search by camera - From the **Camera** drop-down list select the camera that captured the video to search, or leave it set to <any>. If set at <any>, video streams captured from all cameras are searched.

5. Select more search options - More options selected focus the search and return less videos. Keep in mind:

   - For search results to include contiguous video, do not limit your search to a specific NAS device, computer, or unit of media.
   - Drop-down lists support the use of wildcards.

   Select from the options listed below.

| Element | Description |
|---|---|
| **Camera Pool** | If you know a video is located in a specific camera pool, select that camera pool from the drop-down list, type the camera pool name in the box, or use a wildcard.<br><br>A camera pool is a user defined virtual grouping of cameras and can be used to search for video from specified cameras. For example, suppose you have a camera pool called "Doors". It is comprised of all the cameras that watch over the doors of your business. When you need to see who's come or gone, select the "Doors" camera pool as a search criteria, and only video captured from this camera pool are included. There is no limit to the number of camera pools your Phoenix RSM solution may have. |
| **Camera Description** | Limit your search to a specific camera by entering the camera's description. No results are returned if a camera description is not part of the solution. |
| **Show video stored on** | Limit your search to a particular storage device. Select the device from the drop-down list, type the device name, or use a wildcard. |

© 2015

| Element | Description |
|---|---|
| **Show video captured by this computer** | Limit your search to the computer that captured the video. When a computer name is entered, only video stored from that computer is listed. This box may contain only a portion of the computer name, is case sensitive, and allows Wildcards. |
| **Show video stored on this media** | Increase the speed of your search by limiting the search to a particular unit of media. Select the media from the drop-down list, type the media name, or use a wildcard. |
| **Show video stored in this storage pool** | Limit your search to only a specific storage pool. Select the storage pool from the drop-down list, type the storage pool name, or use a wildcard. |

6. Click **Add** for additional search criteria. Add as many search criteria blocks with as much additional criteria as you need to obtain the level of refinement you want. By default, only two extended search criteria are available which are the Any Metadata Field and Content option.

- **Any Metadata Field -** A global metadata search that will match any metadata field. This option is always available.
- **Content** - Search for a word or phrase that is contained in the file or in log entries. This search uses AND boolean logic to get more specific search results.

The available search criteria can be extended through the use of custom metadata. See MetadataExtensions.cfg.

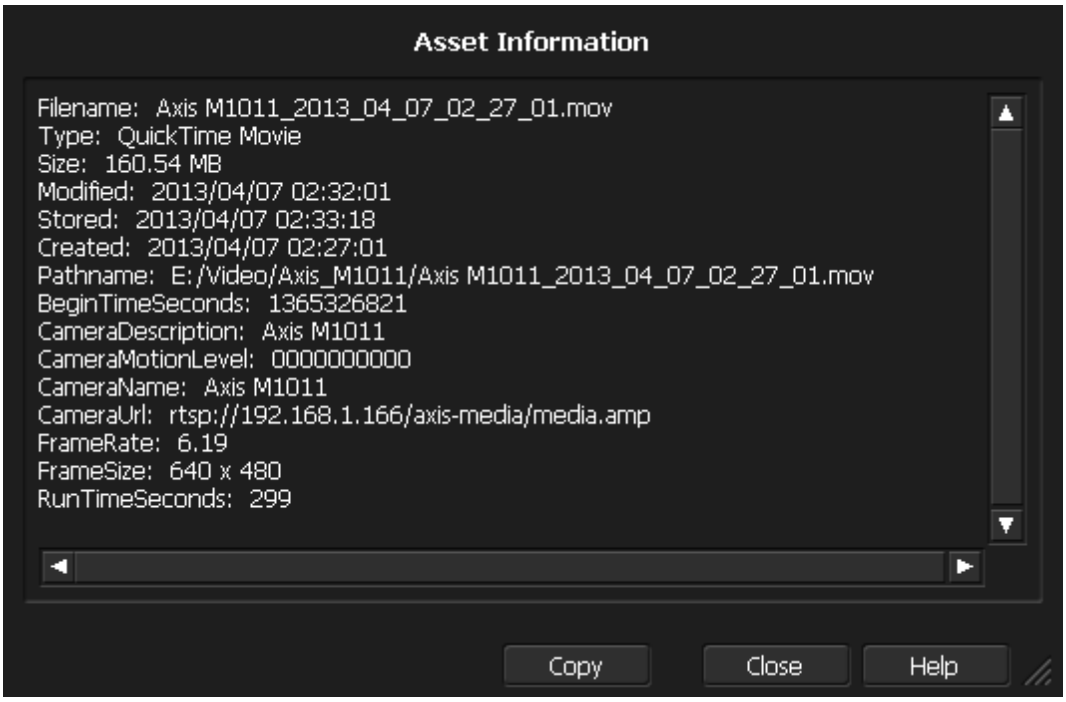
7. After setting search criteria, click the **Search** button to search through the Information Repository for files that match the criteria you have defined. Results, including metadata, appear in the **Search Results** pane.

If a thumbnail is not available, a placeholder image appears as a result. Unless you have selected **Load images immediately when scrolling** in the SVM User Preferences, thumbnail images are loaded only when you stop scrolling.

© 2015

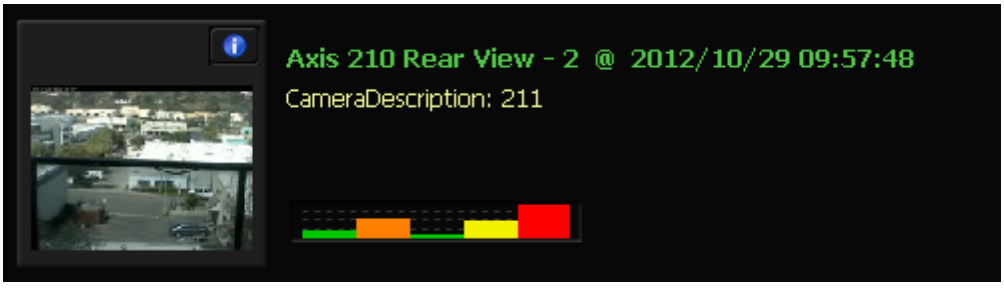
## Search Results

8. In the Search Results pane, click the information icon to the right above the thumbnail to view asset information for the video. In the Asset Information window, various types of information is displayed for the specific video including Filename, Size, Stored date, Camera Name, and many more.




9. In the Search Results pane, double-click the thumbnail image for the file you want to view, or click a point of interest in the histogram. This opens the Media Viewer with the original video file ready for playback and review.

   - Right-click on a thumbnail to choose an action to perform.




The Search Results pane includes the following information (when in Detail view mode):

- A thumbnail image depicting the beginning of the captured video. Surveillance video displays in the Search Results pane from one camera continuously recording. (From Camera Policies Standard mode, the video recording clips are five minutes long each by default.)

© 2015

- Name of the camera that captured the video, the date the video was captured, and the time when the capture began, in bold green text.
- Additional information such as Camera Description, Host, Frame Size, Begin Date, and Run Time.
- A histogram (appearing as a sunken horizontal bar). If a supported motion detection enabled camera has captured motion detection information, the histogram displays where motion detection thresholds were reached. When no motion has reached the detection threshold, or no motion detection data has been gathered, then the histogram is filled black and empty.

Line height and color indicate the magnitude of the motion detected (based on how your motion detection enabled camera is configured). See motion detection.

You can easily skip past sections of video where no motion was detected.

Alternatively, you can right-click on a file and choose from one of the many options in the drop-down list.

| Element | Description |
|---|---|
| **Show Metadata** | Select to show metadata for the selected video or image.<br> Click the information icon to the right above the preview image when in Details view mode to quickly access and edit metadata. |
| **Select All** | Select all of the videos and images in the Search Results. |
| **Unselect all** | Unselect all of the videos and images in the Search Results. |
| **Send to Export Queue** | Send the selected video clip to the Export Queue. This will send the entire video without creating any clips or logs. |
| **Play** | Open the Media Viewer with the selected video queued up and ready to play. |

## Media Viewer

Use the Media Viewer to play back and review videos at variable speeds, navigate to a particular point in a file, clip particular parts of videos for export, and send clips to the Export Queue. For details see SVM Media Viewer.

10. To select a video clip to export, click and drag the timeline pointer to the point where you want the clip for export to begin, and then click the left scissor button. To end the clip, click and drag the timeline pointer to an end point, and then click the right scissor button.

© 2015

After clipping a video, you have the option of creating a log entry that will be associated and exported with that clip. See SVM Logging for more details.

11. Once you have selected the part of the video you want to export, select **Export**. The clip is sent to the Export Queue pane.

## Export Queue

Once a clip is in the Export Queue, you can still change which part of the video to export. Click the video from the Export Queue. The Media Viewer opens again. After you have made your changes, click **Commit** to save changes, and then close the Media Viewer window.

12. You can right-click on a video in the Export Queue and choose from one of the many options in the drop-down list. These options are also available under **Actions** > **Export Queue**.

| Element | Description |
|---|---|
| **Show Metadata** | Select to show metadata for the selected video or image.<br>Click the information icon to the right above the preview image when in Details view mode to quickly access and edit metadata. |
| **Rename Export File** | Select to rename an export file. Type in a new name and click the **Ok** button to save the new name. If no extension is supplied, the correct extension will be appended to the new name. If an extension is entered which is not correct for the content, the correct extension will be appended to the new name. To reset the file back to the original name, click the **Reset** button.<br>An error message will show if you choose to export renamed video clips as **multiple video clips**. To avoid this error, **reset** the video clip names to the original names or choose to export the video clips as a **single video**. |
| **Remove from Export Queue** | Remove the selected video clip from the Export Queue. The removed file is not deleted and will be available for any subsequent searches. |
| **Select All** | Select all of the videos and images in the Search Results. |
| **Unselect all** | Unselect all of the videos and images in the Search Results. |

© 2015

| Element | Description |
|---|---|
| **Play** | Open the Media Viewer with the selected video queued up and ready to play. |

13. When done selecting videos to export and they are in the Export Queue, click the **Export** tab at the top of the main window to activate the export panes. Set the options found in the section Export Surveillance Video to complete the export process.

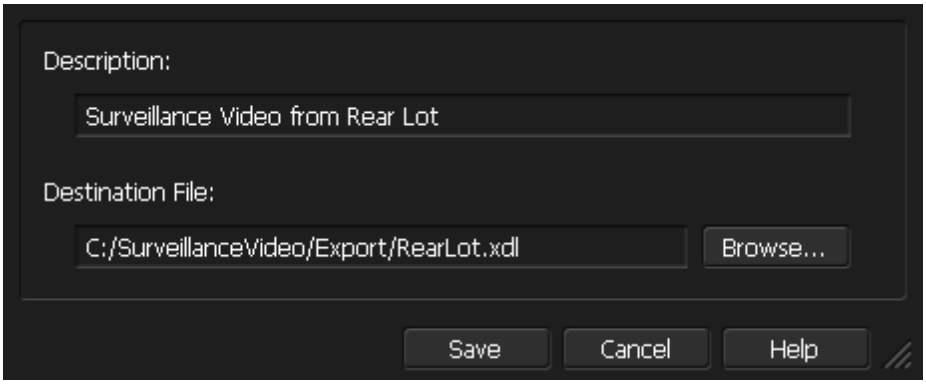
You can save your Export Queue selections for later use. See SVM Save and Load Export Queue.

# SVM Save and Load Export Queue

Being able to save the clip selections that are in the Export Queue is a very useful feature of the Surveillance Video Manager. After searching for video and sending the clips to the Export Queue, you have the option to save the selections to a .xdl file (Export Decision List). Once they have been saved to a file, you can then share the file or load the Export Queue at a later time using the file of saved selections. This means any work in progress can be saved for later use and it allows multiple users to use the same clip selections even though they are working on different machines.

## Save the Export Queue Selections

1. Click **File > Export Queue > Save as**. This will open the Save Export Decision List window.




2. Type a description of the clips in the **Description** text box.
3. Type a pathname in the **Destination File** text box or click **Browse** to open the Choose a File window.
    - If you clicked Browse, navigate to a preferred folder and enter the file name to be saved as in the **File name** text box. Click Open.
4. Click **Save** in the Save Export Decision List window to complete the save process.

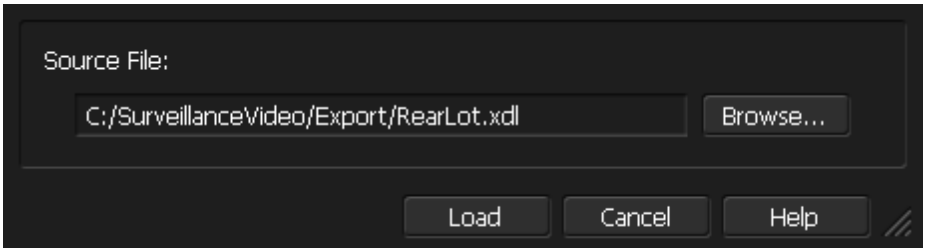
© 2015

### Save Export Decision List window Elements

| Element | Description |
|---|---|
| **Description** | The description of the export decision list.<br>The description is used to provide a quick reference to what is contained in the export decision list. This is optional. |
| **Destination File** | The file to which the export decision list will be saved.<br>Manually enter the pathname of the file or click **Browse** to navigate to a preferred folder and type the file name. |

## Load the Export Queue Selections from a File

1. Select **File > Export Queue > Load from**. This will open the Load Export Decision List window.




2. Type a pathname in the **Source File** text box or click **Browse** to open the Choose a File window.
    - If you clicked Browse, navigate to the .xdl file that was previously saved from the Export Queue. Click **Open**.
3. Click **Load** in the Load Export Decision List window to load the Export Queue from the file.

### Load Export Decision List window Elements

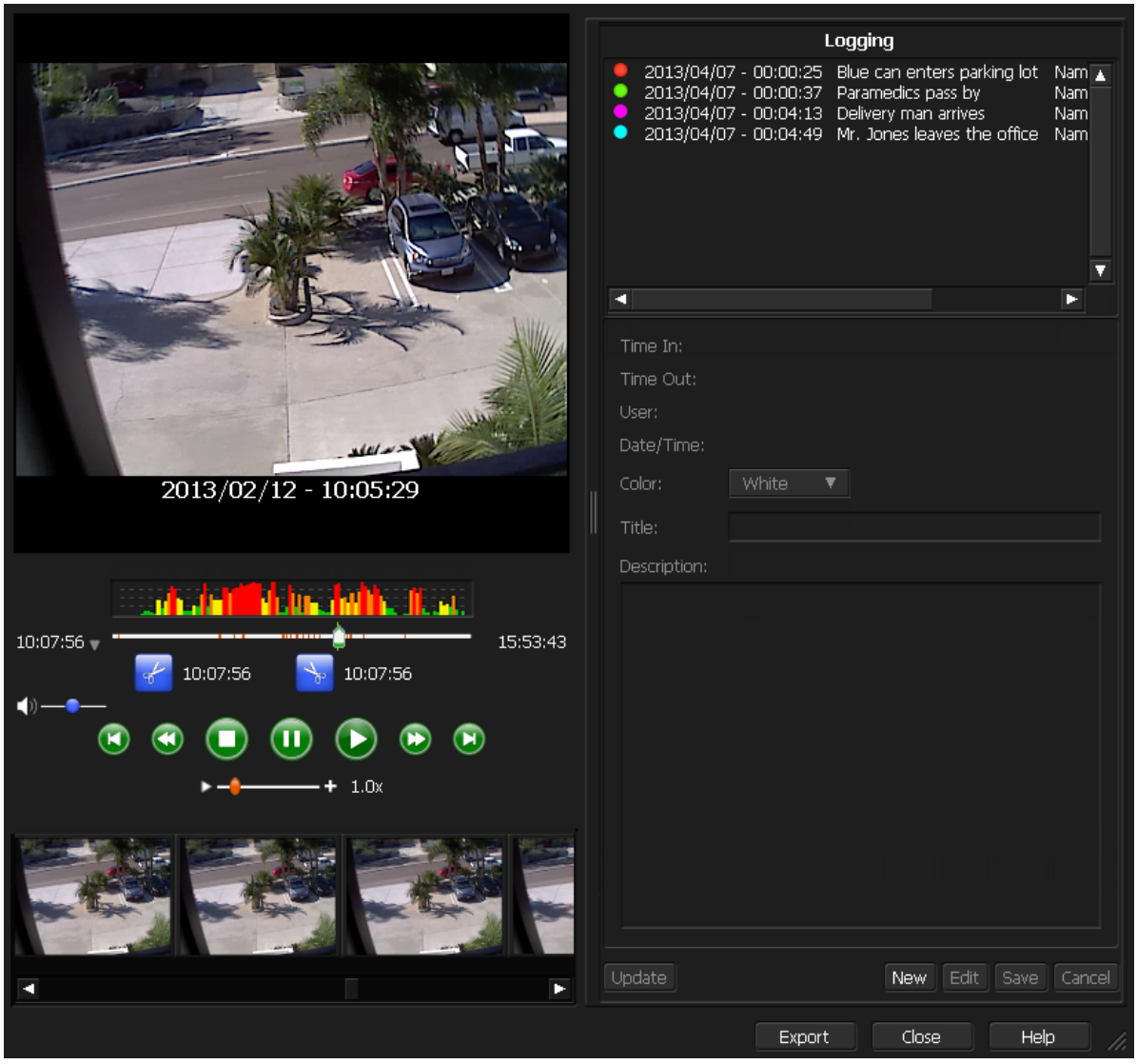
| Element | Description |
|---|---|
| **Source File** | The file from which the export decision list will be loaded.<br>Manually enter the pathname of the file or click **Browse** to navigate to a .xdl file that will be used. |

# SVM Media Viewer and Logging

In the Search Results pane, double-click the file you want to view. The Media Viewer window opens with a low resolution proxy video ready for viewing and all of the log entries for the video are displayed (if any have been created).

© 2015

Remember that low resolution proxy files (also called companion files) are playable videos a fraction of the size of stored originals and are created when data is captured or ingested. They allow for quick retrieval and viewing of stored video. The low resolution proxies remain online, even if their originals are offline. They are entirely managed and fully searchable.




The Media Viewer window is divided into two main areas:

- **Media Viewer -** Use the Media Viewer to view videos at different speeds, search metadata content, navigate to a particular point in a file, clip parts of the video for export, and send clips to the Export Queue. It is comprised of the basic controls of any popular video viewer (such as volume, play, stop, skip forward, skip back, beginning, and end) and the following additional controls: timeline, scissors, jog shuttle, playback speed, search box, and storyboard.

© 2015

- **Logging -** The logging area of the Media Viewer is used to create logs about specific clips of a video. At the top of this area is a list of all the saved log entries for the selected video. When a log entry has been selected, information on the clip is displayed such as time in and time out, and it provides information about the selected log such as the user who created it, date and time created, bullet color associated with the clip, and the title and description of the clip. The entire Logging panel can be minimized for maximum media viewer viewing, or the panel can be maximized to manage the log entries.

For more information, see SVM Media Viewerand SVM Logging.

## SVM Media Viewer

The left side of the Media Viewer window is the actual **Media Viewer**. When the Media Viewer opens, the low resolution proxy video is queued up for viewing (if the proxy video generation was enabled when the video was captured). If no low resolution proxy video is available, the original video file is played. Use the Media Viewer to view videos at different speeds, search metadata content, navigate to a particular point in a file, clip parts of the video for export, and send clips to the Export Queue. It is comprised of the basic controls of any popular video viewer (such as volume, play, stop, skip forward, skip back, beginning, and end) and the following additional controls:

Remember that low resolution companion files (also called proxy files) are playable videos a fraction of the size of stored originals and are created when data is captured or ingested. They allow for quick retrieval and viewing of stored video. The low resolution companions remain online, even if their originals are offline. They are entirely managed and fully searchable.

© 2015

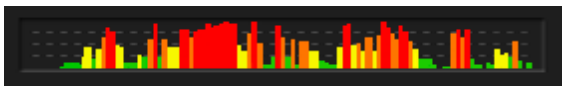
The Media Viewer is comprised of the controls in any popular video viewer (such as volume, play, stop, skip forward, skip back, beginning, and end) and the following additional controls:

© 2015

A few things to note about the SVM Media Viewer:

- The histogram in the Media Viewer is different from the one on the Surveillance Video Manager Search Results pane in that it represents all of the found videos for the one particular camera selected from the Search Results pane.
- When a video clip is selected from the Search Results pane, the Media Viewer allows playback and review of the entire timeline that was specified from the Search Criteria pane - not just the recorded clip generated, which by default is five minutes long. For example, with a date range of July 20 to July 26, you may have a large number of thumbnail Search Results to choose from. Once you click a thumbnail item, a Media Viewer displays all video from July 20 to July 26 for the camera associated to the thumbnail selected.
- The Media Viewer offers great flexibility to search back and forth within the video timeline and to view the histogram associated to the timeline of a selected camera. The pointer on the timeline is located where the video clip selected appears along the timeline.
- Multiple Media Viewer can be opened at once, each depicting the entire timeline associated to the Search Criteria date and time requested. If the Media Viewer is left open and another thumbnail is selected from the same camera, the pointer on the timeline shifts to the new time. If a thumbnail is selected from a different camera, then a new Media Viewer opens.

## Histogram



The histogram in the Media Viewer spans video recorded from one camera (not just one video segment from the camera). This is useful for you to quickly view portions of the video with the most interest. The histogram appears as a sunken horizontal bar, and if a supported motion detection enabled camera has captured motion detection information, the histogram displays where motion detection thresholds were reached. When no motion has reached the detection threshold, or no motion detection data has been gathered, then the histogram is filled black and empty.

Line height and color indicate the magnitude of the motion detected (based on how your motion detection enabled camera is configured). See motion detection.

## Timeline

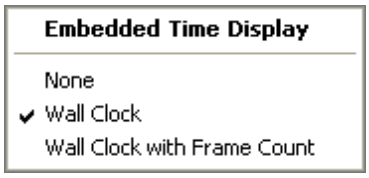
The timeline pointer indicates the part of the video that is displayed. Click, hold, and drag the pointer either forward or backward in the video. Click to the left of the pointer to rewind the video one second at a time, or click to the right of the pointer to advance the video one second at a time. Click and hold in either direction, and the pointer moves automatically one second at a time.

© 2015

The number to the left is a time code that indicates where the pointer is in the video (and the part being displayed). The number to the right indicates the total length of the video. The vertical green line to the left indicates where a clip begins, and the vertical green line to the right indicates where a clip ends. Only the segment of video between the vertical green lines will be exported. By default, the lines mark the beginning and the end of the video; they can be adjusted using the scissor buttons.

If you set the beginning of the clip to within one second of the beginning of the file and one second of the end of the file, the entire original full resolution file is exported.

Some video includes an embedded time display, or time code, that assigns a number to each video frame of video. This is indicated by a golden triangle in the timeline. Click the triangle to select an embedded time display option.




## Scissors

Use the scissor buttons to select clips from the video. Numbers indicate beginning and ending times. Click the left button to denote the beginning of the clip, and the right button to denote the end of the clip. You can repeat this process to export as many clips from a video as you need; this creates multiple clips from a single file. However, before selecting and exporting a second clip, you need to add the currently selected clip to the export queue by clicking the **Export** button on the main Media Viewer window.

## Playback Speed

Use the playback speed to run the video faster or slower. Drag the orange control to the left to play more slowly or to the right to play more quickly.

## Storyboard

© 2015

The Storyboard strip at the bottom of the Media Viewer displays still images taken from the video file. It provides a visual representation of the video file contents and an easy way to quickly see and navigate to a point of interest in the video. Use the horizontal scrollbar to scroll through the frames. As you move your mouse over an image, the time associated with the image is displayed. Click an image to jump to that point in the video, and note that the pointer jumps to the corresponding point on the timeline.

### Keyboard Navigation

The Media Viewer also supports the following case sensitive keyboard navigation:

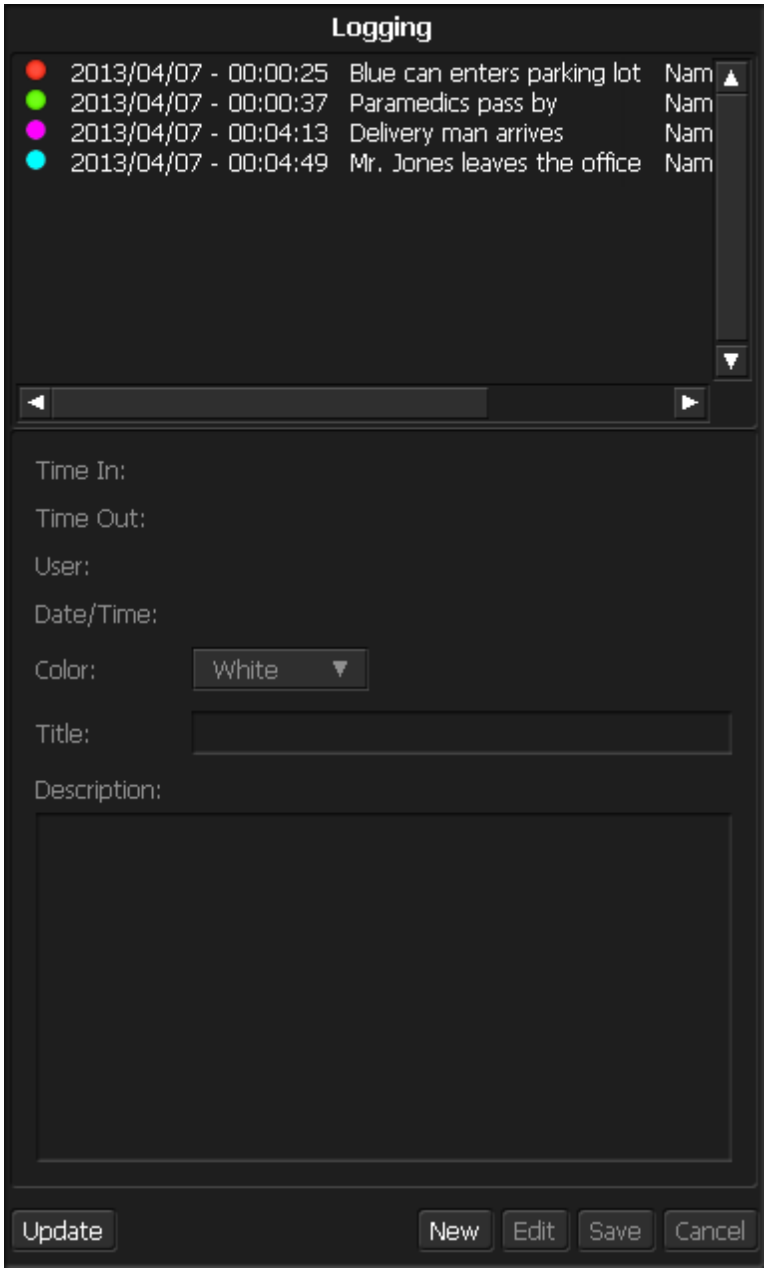
| Action | Key Combination |
|---|---|
| Frame-by-frame forward | ALT + RIGHT ARROW |
| Frame-by-frame backward | ALT + LEFT ARROW |
| Move one second forward | RIGHT ARROW |
| Move one second backward | LEFT ARROW |
| Skip forward 30 seconds | SHIFT + RIGHT ARROW |
| Skip backwards 30 seconds | SHIFT + LEFT ARROW |
| Toggle play/pause | SPACE BAR |
| Skip to "in" point | SHIFT + I |
| Skip to "out" point | SHIFT + O |
| Set "in" point | I |
| Set "out" point | O |
| Increase playback speed | J |
| Decrease playback speed | L |
| Stop playback | K |

For more information see Search Surveillance Video and Surveillance Video Manager.

© 2015

## SVM Logging

The right side of the Media Viewer window is the **Logging** panel. Creating log entries for specific clips allows a user to add and save notes about the content of the video that is being viewed. These notes are turned into logs which are grouped together and associated with the selected video. Each log can be saved as a simple text file that can be used and viewed even if the Media Viewer is not available. Any user can edit, add, and delete logs even if they were not the original user to create them. This allows for multiple users to work on a project and save all of the work together in a single location. Once logs have been created, they become searchable content and can be entered as search criteria in the main Search tab of the Surveillance Video Manager.




© 2015

## List of Log Entries

This list displays each log entry and is organized chronologically according to the clip start time. Each entry in the list will have a colored bullet, the start date and time of the clip, the title, and the user who created the log entry. Select a log from this list to display all of its information and to view, edit, or delete it.

Logging
2013/04/07 - 00:00:25 Blue can enters parking lot Nam
2013/04/07 - 00:00:37 Paramedics pass by Nam
2013/04/07 - 00:04:13 Delivery man arrives Nam
2013/04/07 - 00:04:49 Mr. Jones leaves the office Nam

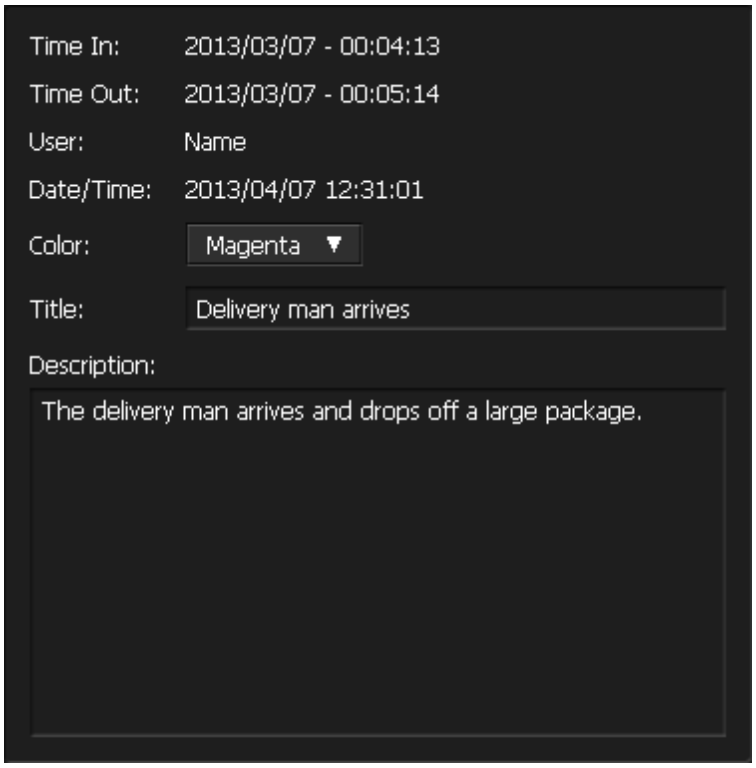
To access the shortcut controls for managing the list of log entries, right-click on a selected entry. Select from the following options:

- **New** - Create a new log entry.
- **Edit** - Edit the selected log entry.
- **Delete -** Delete the selected log entry.
- **Export** - Send the log entry and the clip associated with it to the Export Queue.
- **Save As** - Save the log entry as a text file (.txt). This file will contain all of the basic information about the log entry and can be viewed independent of the video clip.

## Information about Selected Log Entry

The information displayed about a selected log includes information about the clip and notes about the content.

© 2015




## Logging Panel Elements

| Element | Description |
|---|---|
| **Time In** | The beginning time of the clip. This value has both the calendar date and wall clock time for that clip.<br><br>This value can be changed by using the left scissors button in the Media Viewer. |
| **Time Out** | The end time of the clip. This value has both the calendar date and wall clock time for that clip.<br><br>This value can be changed by using the right scissors button in the Media Viewer. |
| **User** | The user who created the log entry. |
| **Date/Time** | Year/Month/Day and time that the log entry was created or last edited.<br><br>The date and time will be updated when the log entry is edited and then saved. |
| **Color** | The color of the bullets associated with the clip and log entry. |

© 2015

| Element | Description |
|---|---|
| | Each log entry has a corresponding bullet color that can be used to visually associate related clips. Choose from White, Red, Yellow, Green, Cyan, Blue, Magenta, or Black. |
| **Title** | The title of the clip and log entry.<br><br>A user can change this value by typing a new title in the text box. The title will be displayed in the list of log entries at the top of the Logging panel and is searchable content in the search criteria tab of the Surveillance Video Manager. |
| **Description** | The description of the clip and log entry.<br><br>The description is optional. A user can change this value by typing a new description in the text box. The description is searchable content in the search criteria tab of the Surveillance Video Manager. |

## Create a New log entry

After you have created a clip using the Media Viewer scissors and controls, you can create a log entry to keep track of any notes that you wish to add.

1. Click **New**.
2. Change the Time In and Time Out values by using the scissors in the Media Viewer.
3. Choose a color from the **Color** drop-down list.
4. Enter a title of the clip in the **Title** text box.
5. Enter a description of the clip in the **Description** text box.
6. Click **Save**.

In order to get better search results for clips that have log entries associated with them, turn on **Search for preview images**, **Search for low resolution proxies**, and **Search for related files** in User Preferences.

## Edit a log entry

Any log entry that is displayed in the list can be edited.

1. Select a log entry that you want to edit.
2. Click **Edit**. All of the information contained in that log will be displayed.
3. Edit the information and then click **Save**.

© 2015

- Editing information is done similarly to steps 2 - 6 in the above directions about how to create a log entry.

User and Date/Time are not available for direct editing. Date/Time will change after a log entry has been edited and then saved.

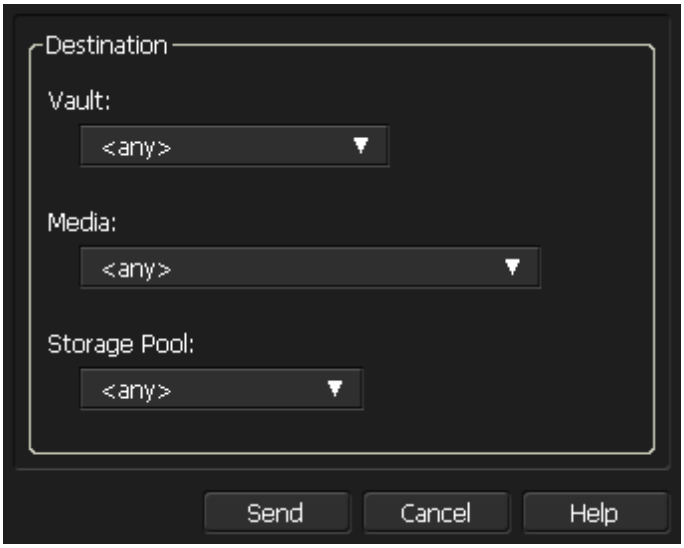
## Delete a log entry

1. Select a log entry from the list that you want to delete.
2. Right-click on that entry and select **Delete** from the shortcut menu.

## Update the Repository with log changes

The Information Repository needs to be updated with any changes that have been made to logs.

1. Click **Update**. The Send Logging Information window opens.




2. Choose a value from the **Vault**, **Media**, and **Storage Pool** drop-down lists.
   - You can specify as many as you like or leave them as <any>.
3. Click **Send** to send these changes to the Repository.

## Send Logging Information window Elements

| Element | Description |
|---|---|
| **Vault** | From the drop-down list, select a Vault or select **<any>** to use any available vault. |

© 2015

| Element | Description |
|---|---|
| | If a Vault is selected, the Media and Storage Pool drop-down lists are automatically populated with the media and storage pools on the given Vault.<br><br>If <any> is selected, then the Media and Storage Pool options contain all available media and storage pools. |
| **Media** | Media refers to the names of individual units of media in the Vaults within the Information Repository.<br><br>From the drop-down list, select the media or select **<any>** to use any available vault. The system automatically looks for any storage pools comprised of the selected media. If it cannot find any, then the Storage Pool drop-down list displays <any>. |
| **Storage Pool** | Storage pools are groupings of media on a single policy used for a particular purpose. For example, if you had a policy called "Night backup" and it wrote to several units of media, you would use a "Night backup" storage pool and assign to it every unit of media to use for that purpose. For more information see Prepare Media, Storage Pool.<br><br>From the drop-down list, select a storage pool or select **<any>** to use any available storage pool. |

For more information see Search Surveillance Video and Surveillance Video Manager.

# Export Surveillance Video

After you have searched for, reviewed, and selected the video clips to export from the Surveillance Video Manager **Search** tab and the videos are in the Export Queue, use the Surveillance Video Manager **Export** tab to export the video in different ways.

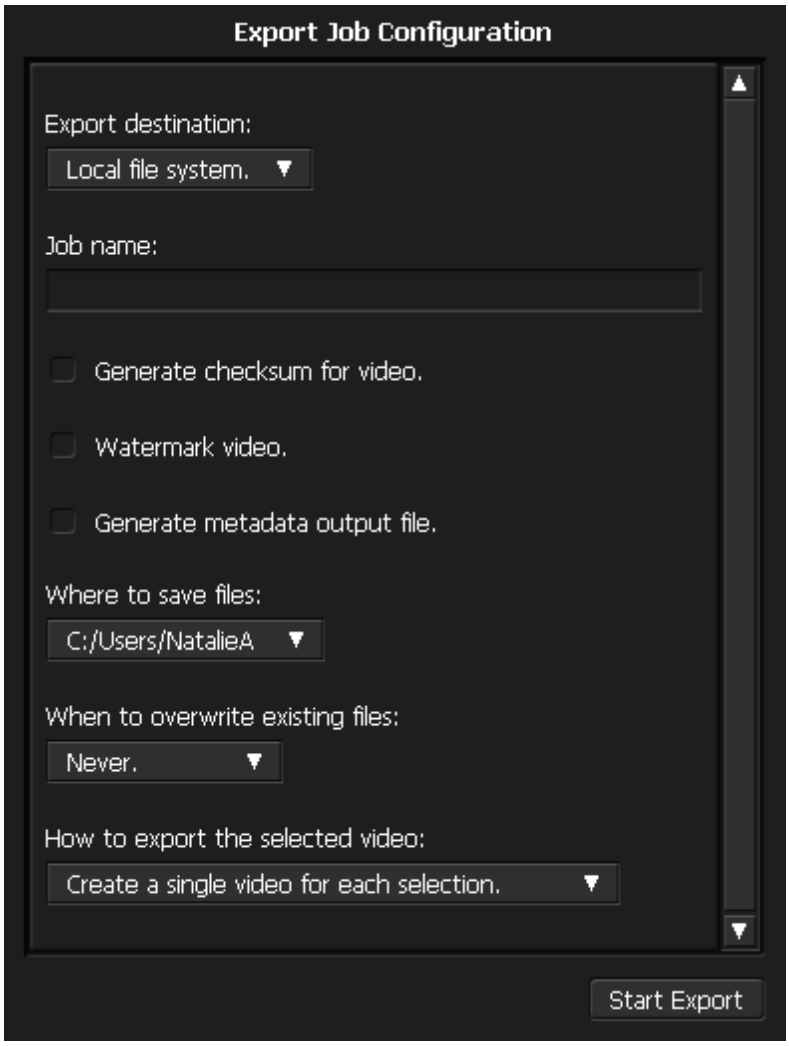
Access the Export window panes by clicking the **Export** tab at the top of the main Surveillance Video Manager application window.

Depending on your system, the following options may or may not be available for you to select from. The contents in the Export Job Configuration pane are dynamic depending on the **Export Destination** chosen. Work your way through the Export Job Configuration pane parameters.

## Local File System

The **Export Destination** of local file system is the default setting for this pane. Populate the options when **Local File System** is selected.

© 2015




| Element | Description |
|---|---|
| **Export destination** | Define where files are exported to. (Local File System.) |
| **Job name** | Type a job name to associate a text name with the job. This name appears in job logs. |
| **Generate checksum for video** | Select to generate a checksum file for each exported video file. The checksum (or digital fingerprint) is calculated using the SHA256 hash algorithm. The resulting filename is the original base name with a .sha256 extension. |
| **Watermark video** | Select to apply a watermark to the exported video file. When this item is selected, the pane expands to show additional fields. |

© 2015

| Element | Description |
|---|---|
| | **Placement** - Specify where the watermark should be placed in the video. Select from upper left, upper right, lower left, lower right, and center.<br><br>**Type** - Specify the type of watermark to be applied. If **Text**, then there are fields displayed to input the text size, text color, and the actual text to be used as the watermark. If **Bitmap**, then a box displays where the pathname of a watermark file can be entered, or click the **Browse** button to browse for the watermark file.<br><br> When using QuickTime as the backend to watermark a video, the preferred format for a watermark file is Portable Network Graphics (.png extension). If you use a bitmap (.bmp) file, the watermark image will not be transparent and it will be surrounded by a white box covering up part of the video. |
| **Generate metadata output file** | Generate metadata xml files for output along with video. If selected, a drop-down list appears for you to select **Create multiple files** or **Create a single file**.<br><br>• **Create multiple files** - The metadata file has the same name as its associated video file, but with the . xml extension. One metadata file per video is created and they stick together.<br><br>• **Create a single file** - A single file containing the metadata for all files being exported is generated. A Metadata output file box appears, requiring a name for the metadata file. Click the **Browse** button to select.<br><br>At a minimum the data included contain pathname, file id, size, and the date and time modified. |
| **Where to save files** | Export data back to its original location or to any other location on the network.<br><br>**Original location** - Export data to its original location.<br><br>**Different location** - Export data to another location. Use the Browse For Folder window to select the location, and click **OK**. |
| **When to overwrite existing files** | Select an option of **Never**, **Only if newer**, or **Always**, outlining when to overwrite files. |

© 2015

| Element | Description |
|---|---|
| | If the files exported already reside in some form on the target computer - that is a conflict and the export job does not work. |
| **How to export the selected video** | With several clips captured from the same camera, select export them as a single video or multiple video clips for each selection.<br><br>An error message will show if you choose to export renamed video clips as **multiple video clips**. To avoid this error, **reset** the video clip names to the original names or choose to export the video clips as a **single video**. |

## Rimage

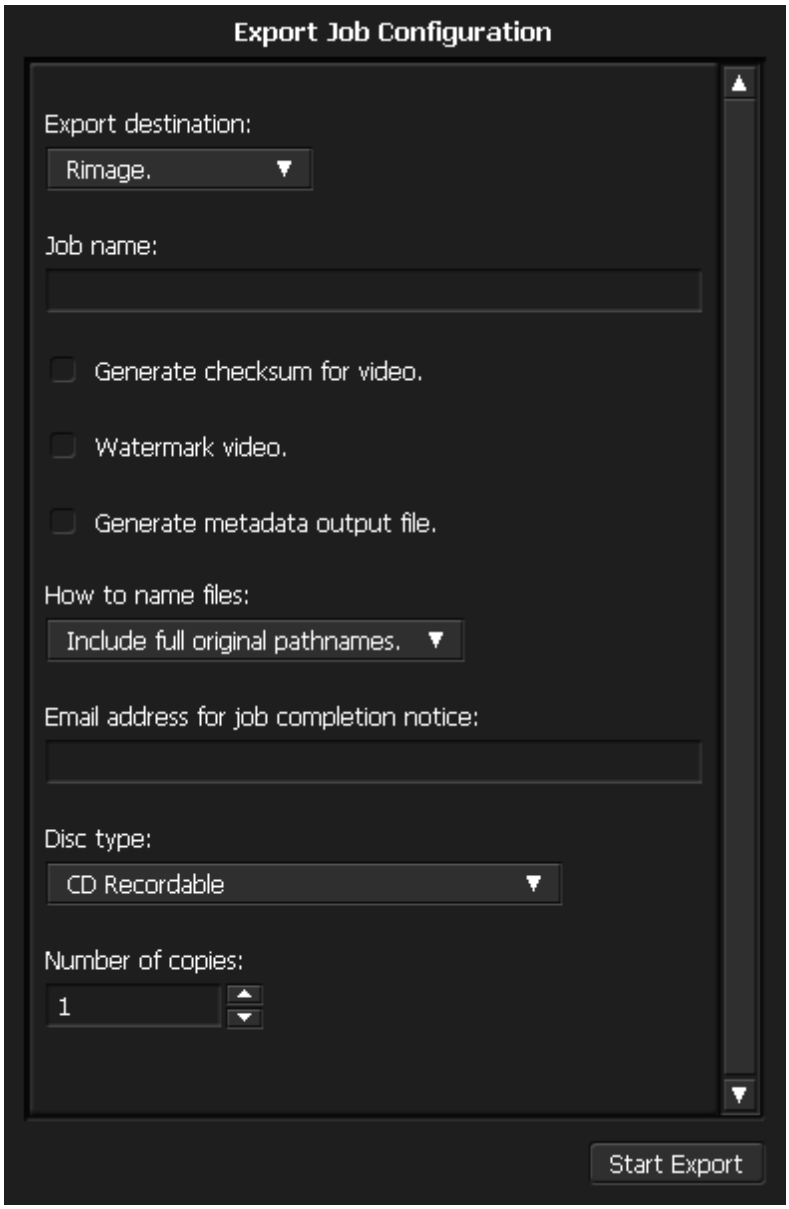
Populate the options when **Rimage** is selected.

Export to Rimage only works if your Rimage system and Phoenix RSM export are configured properly.

When exporting to the Rimage, do not stop Phoenix RSM until all jobs have finished. If you do, temporary files are not removed and those files will have to be removed manually. To manually remove temporary files, go to the Rimage Export Folder, and remove <user name>_<uuid>.

For more information see Rimage Configuration window.

© 2015




| Element | Description |
|---|---|
| **Export destination** | Define where files are exported to. (Rimage.)<br><br>This option is only available when it is enabled in your User Preferences. |
| **Job name** | Type a job name to associate a text name with the job. This name appears in job logs. |

© 2015

| Element | Description |
|---|---|
| **Generate checksum for video** | Select to generate a checksum file for each exported video file. The checksum (or digital fingerprint) is calculated using the SHA256 hash algorithm. The resulting filename is the original base name with a .sha256 extension. |
| **Watermark video** | Select to apply a watermark to the exported video file. When this item is selected, the pane expands to show additional fields.<br><br>**Placement** - Specify where the watermark should be placed in the video. Select from upper left, upper right, lower left, lower right, and center.<br><br>**Type** - Specify the type of watermark to be applied. If **Text**, then there are fields displayed to input the text size, text color, and the actual text to be used as the watermark. If **Bitmap**, then a box displays where the pathname of a watermark file can be entered, or click the **Browse** button to browse for the watermark file.<br><br> When using QuickTime as the backend to watermark a video, the preferred format for a watermark file is Portable Network Graphics (.png extension). If you use a bitmap (.bmp) file, the watermark image will not be transparent and it will be surrounded by a white box covering up part of the video. |
| **Generate metadata output file** | Generate metadata xml files for output along with video. If selected, a drop-down list appears for you to select **Create multiple files** or **Create a single file**.<br><br>• **Create multiple files** - The metadata file has the same name as its associated video file, but with the .xml extension. One metadata file per video is created and they stick together.<br><br>• **Create a single file** - A single file containing the metadata for all files being exported is generated. A Metadata output file box appears, requiring a name for the metadata file. Click the **Browse** button to select.<br><br>At a minimum the data included contain pathname, file id, size, and the date and time modified. |
| **How to name files** | Define how selected data is arranged when retrieved. There are three options: |

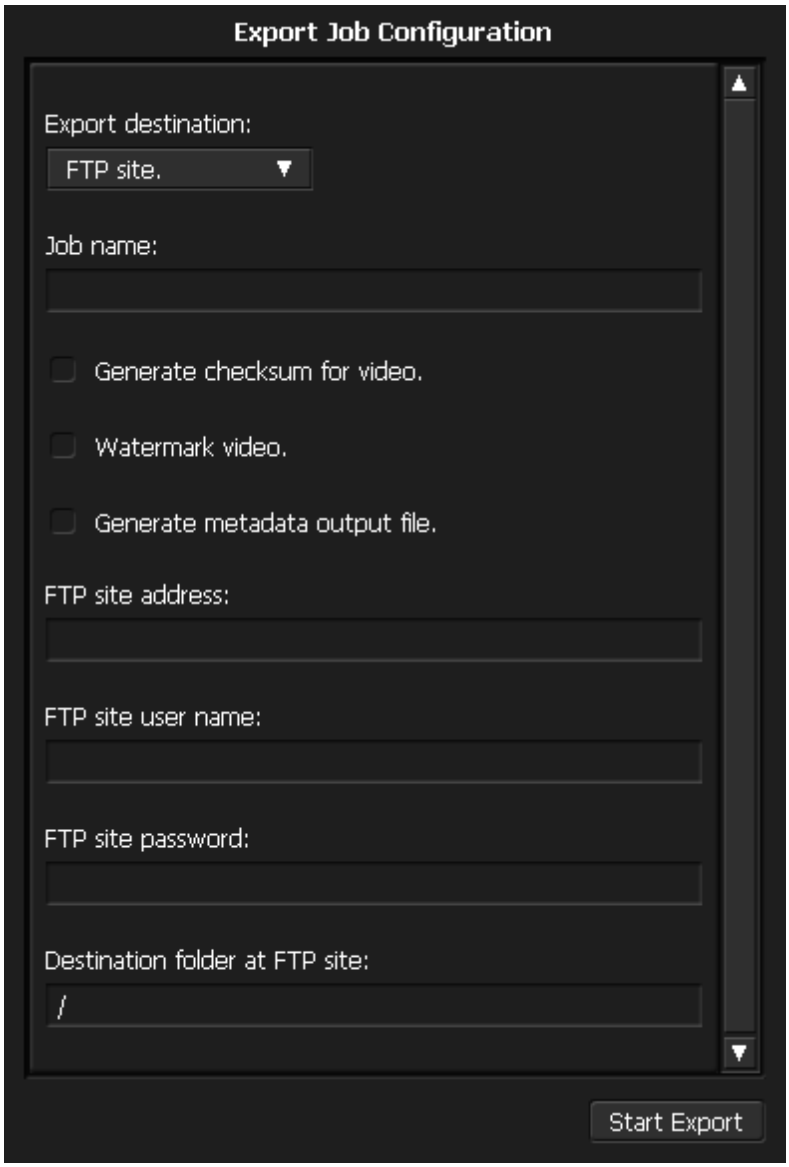
© 2015

| Element | Description |
|---|---|
| **Active only for Different Location and Export to Rimage**. | **Include full original pathnames** - This option recreates the source file structure. The retrieved data file structure matches that of the source file. For example, if the source is "C:\Accounting\Marketing\...", then the retrieved data is "C\Accounting\Marketing\...".<br><br>**Include filenames only** - This option ignores file folders, and the retrieved data is comprised of only files.<br><br> **Include filenames only** do not work correctly if selected files have identical names. When working with identical names, use **Include full original pathnames** or **Include pathnames starting at selected items**. |
| **E-mail address for job completion notice** | Type a valid e-mail address to define where Rimage sends an e-mail when the Rimage job is finished. |
| **Disc type** | Define the type of media for Rimage to make. |
| **Number of copies** | Define how many copies of the data for Rimage to make. Press TAB or ENTER for the new number typed to take effect. |
| **Disc labeling** | Define the information on media labels for the media that Rimage is producing.<br><br>The number and titles of the fields available depend on what is entered in the Rimage Configuration window.<br><br>If a field is not present, add it using the Rimage Configuration window. |

## FTP Site

Populate the options when FTP Site is selected.

© 2015




| Element | Description |
|---|---|
| **Export destination** | Define where files are exported to. (FTP site.)<br><br>This option is only available when it is enabled in your User Preferences. |
| **Job name** | Type a job name to associate a text name with the job. This name appears in job logs. |

© 2015

| Element | Description |
|---|---|
| **Generate checksum for video** | Select to generate a checksum file for each exported video file. The checksum (or digital fingerprint) is calculated using the SHA256 hash algorithm. The resulting filename is the original base name with a .sha256 extension. |
| **Watermark video** | Select to apply a watermark to the exported video file. When this item is selected, the pane expands to show additional fields.<br><br>**Placement** - Specify where the watermark should be placed in the video. Select from upper left, upper right, lower left, lower right, and center.<br><br>**Type** - Specify the type of watermark to be applied. If **Text**, then there are fields displayed to input the text size, text color, and the actual text to be used as the watermark. If **Bitmap**, then a box displays where the pathname of a watermark file can be entered, or click the **Browse** button to browse for the watermark file.<br><br> When using QuickTime as the backend to watermark a video, the preferred format for a watermark file is Portable Network Graphics (.png extension). If you use a bitmap (.bmp) file, the watermark image will not be transparent and it will be surrounded by a white box covering up part of the video. |
| **Generate metadata output file** | Generate metadata xml files for output along with video. If selected, a drop-down list appears for you to select **Create multiple files** or **Create a single file**.<br><br>• **Create multiple files** - The metadata file has the same name as its associated video file, but with the .xml extension. One metadata file per video is created and they stick together.<br><br>• **Create a single file** - A single file containing the metadata for all files being exported is generated. A Metadata output file box appears, requiring a name for the metadata file. Click the **Browse** button to select.<br><br>At a minimum the data included contain pathname, file id, size, and the date and time modified |
| **FTP site address** | Type the host name or address. |
| **FTP site user name** | Type the user name to log into the FTP site. |

© 2015

| Element | Description |
|---|---|
| **FTP site password** | Type the password to log into the FTP site. |
| **Destination folder at FTP site** | Type the destination path and directory the files should be exported to. This directory is a place to store files. |

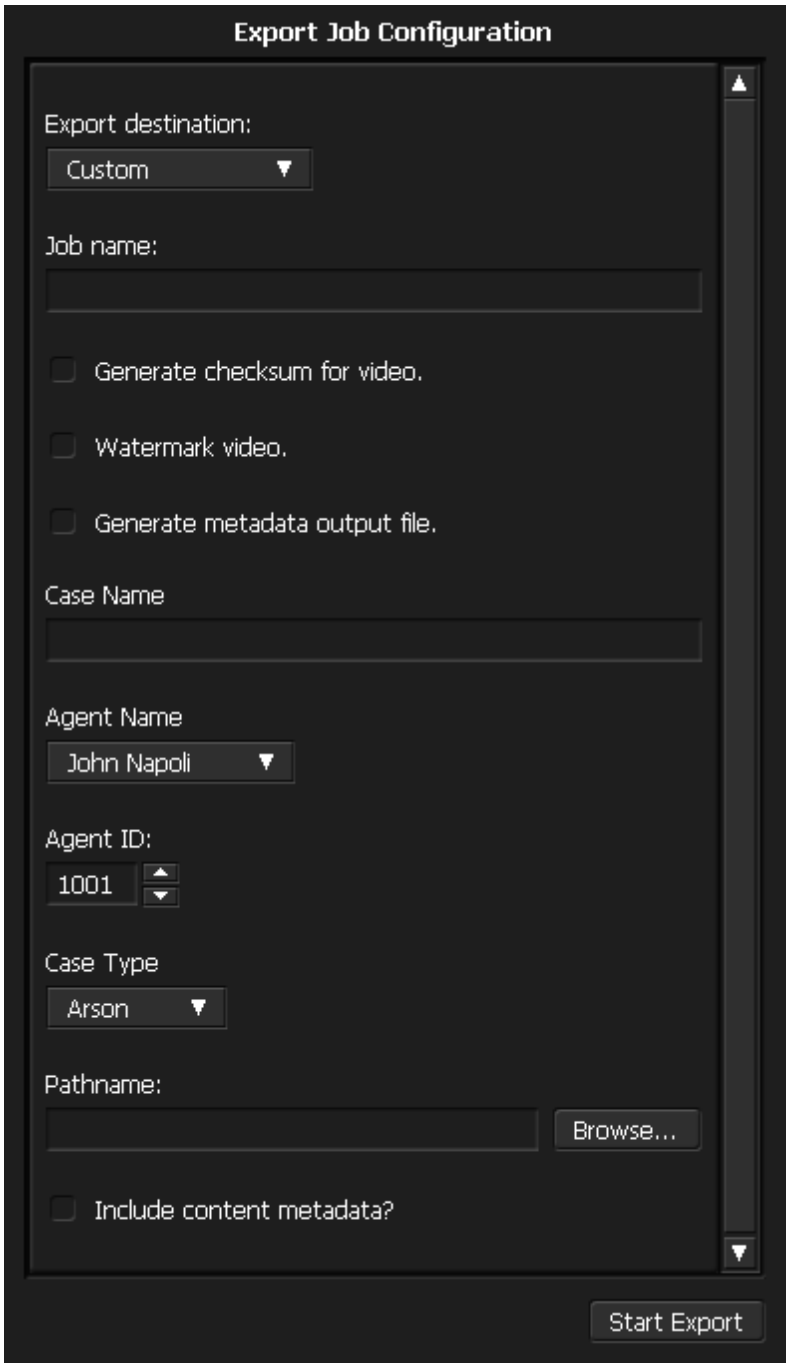
## Custom

You can customize export options for **Export Job Configuration**. Custom options are available only when an ExportExtensions.cfg file is in place.

Available options are customizable via ExportExtensions.cfg at <install-dir>\Program Files\Phoenix\Config.

For more information see ExportExtensions.cfg.

© 2015




| Element | Description |
|---|---|
| **Export destination** | Define where files are exported to. (Custom.) |
| **Argument <1 - 8>** | These fields are defined in ExportExtensions.cfg by your Phoenix RSM administrator. Consult your Phoenix RSM administrator for details. |

© 2015

| Element | Description |
|---|---|
| | The image above displays the arguments from a sample ExportExtentions.cfg file.<br>• Blank fields are ignored.<br>• If typing a number into a spin control manually, press TAB or ENTER for the new number to take effect. |

After setting the parameters, click **Start Export** to export videos. A job status box appears in the Job Status pane during the job, and the **Stop** button is active.

If you click **Stop** while it is exporting files, not all of the files in the Export Queue are exported. Any files that have completed export remain on the target computer. Click **Dismiss** to close the job status box.

Click **View** to open a log file for job details or to diagnose export issues.

### Problems with exporting videos?

Existing files on networked computers are not overwritten, by default. If an export job is unsuccessful, there may already be a copy of the files on the target computer. Avoid errors by setting additional export parameters. For example, to overwrite files on a networked computer, from the **When to overwrite existing files** field, select **Always** or **Only if newer**.

- Ensure that the files to overwrite are not write protected by the operating system on the targeted computer.
- From the **When to overwrite existing files** field in the Export Job Configuration pane, select **Always**.
- Click **Start Export** to retry exporting video.

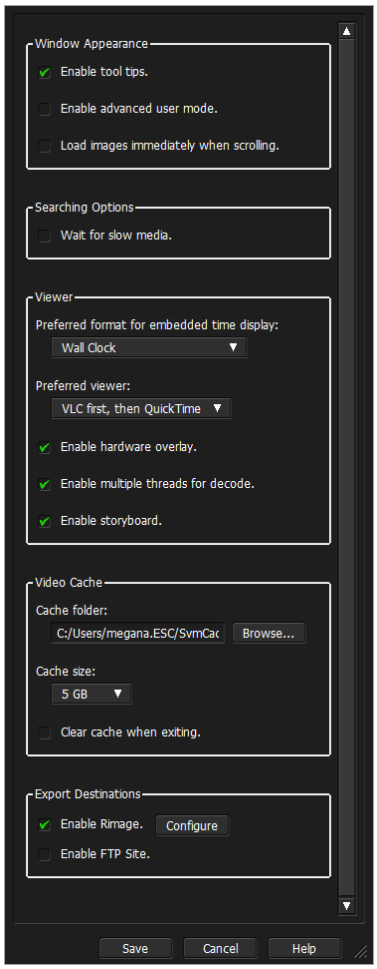
For more information see Search Surveillance Video and Surveillance Video Manager.

## SVM User Preferences

Use the Surveillance Video Manager User Preferences to define default settings for the **Search** and **Export** tabs of the Surveillance Video Manager.

Access the Surveillance Video Manager User Preferences from the Surveillance Video Manager **Tools** menu, select **User Preferences**.

© 2015




## Surveillance Video Manager User Preference Elements

| Group | Element | Description |
|---|---|---|
| **Window Appearance** | **Enable tool tips** | A check mark by this element indicates that tool tips for the Surveillance Video Manager will display. De-select to turn tool tips off. |
| | **Enable advanced user mode** | Select to view advanced information such as run time, size, and frame size in the Search Results pane for each video clip.<br><br>This advanced information may not be visible depending on the version of your software. |
| | **Load images immediately when scrolling** | When checked, thumbnail images are loaded as you scroll down the Search Results pane. If de-selected, thumbnail images load only when scrolling stops. |

© 2015

| Group | Element | Description |
|---|---|---|
| **Searching Options** | **Wait for slow media** | The application will try to retrieve thumbnail images, event entries, logging entries, and other display-related files from slow media, *i.e.* tape. Search results will be slow. Thumbnails only exist on tape or other slow media. |
| **Viewer** | **Preferred format for embedded time display** | Select the type of time code that displays in the Media Viewer. |
| | **Preferred viewer** | Select the type of video viewer to drive the play back of videos. The orders to use the media player are: **QuickTime first, then VLC** , **QuickTime only**, **VLC first, then QuickTime**, or **VLC only**.<br> To play back videos in Phoenix RSM, you can use the supplied media player (VLC) or Apple QuickTime free or Pro on your computer. See Hardware and Software Requirements for the latest information.<br> Be sure to restart any media viewer that is running if you change the preferred viewer. |
| | **Enable hardware overlay** | Select to enable the ability to render video directly.<br> If disabled, remote desktop or shared desktop view may not work correctly for viewing live video streams. |
| | **Enable multiple threads for decode** | Select to be able to use multiple threads and multiple cores for decoding to provide faster decoding of the video.<br> If decoding is not occurring properly, disabling this feature may fix the problem. |

© 2015

| Group | Element | Description |
|---|---|---|
| | **Enable storyboard** | Select to display a storyboard strip in the Media Viewer. The storyboard displays still images from the video. Click an image to jump to that point in the video. |
| **Video Cache** | **Cache folder** | Define the folder where Phoenix RSM caches search results. Similar to the cache of a web browser, the cache stores found thumbnails, low resolution proxy companion videos, and other associated files and enables you to replay already found videos more quickly. Click the **Browse** button to browse for a folder. |
| | **Cache size** | Define the size of the cache where Phoenix RSM caches thumbnails, low resolution companion videos, and associated files. When full, contents overwrite in the order of oldest to newest.<br> If unsure about cache size, leave it set to the default value. If you find that Phoenix RSM often needs to retrieve videos from storage rather than from the cache, increase the cache size. |
| | **Clear cache when exiting** | Select for Phoenix RSM to empty the cache when the application closes. |
| **Export Destinations** | **Export destinations** | Only the export destinations available for the application are displayed. Depending on your product, you may see options to:<br>• **Enable Rimage** - Select to enable the **Configure** button. Use the Rimage Export Configuration window for configuring Rimage to publish video files. (See the following section.)<br>• **Enable Ftp Site**<br>The options selected are then displayed on the **Export** tab > Export Job Configuration pane > in the **Export Destination** drop-down list. The Local File System selection is always available. |
| **Save** | | Save your settings. |

© 2015

| Group | Element | Description |
|---|---|---|
| **Cancel** | | Close the window without saving modifications. |
| **Help** | | Open help. |

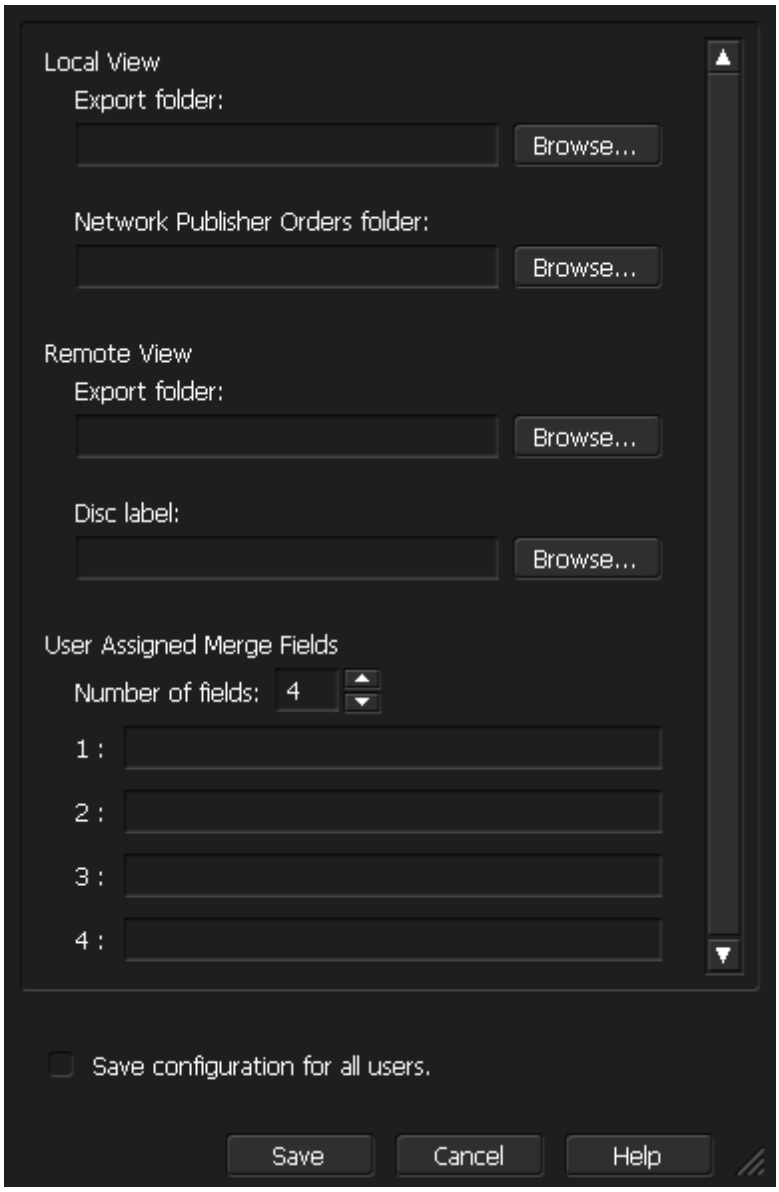
For more information see SVM Search and Export, SVM Media Viewer, and Surveillance Video Manager.

## Rimage Configuration window

Configure for Rimage export using the Rimage Configuration window. This process enables you to export or save files to a Rimage system.

Access the Rimage Configuration window from the User Preferences window. Under **Export Destination**, select **Enable Rimage**, and then click the **Configure** button.

© 2015




| Element | Description |
|---|---|
| **Local View: Export folder** | The view of the export folder on the Phoenix RSM client computer from the client computer. The client computer refers to the computer where Phoenix RSM is running.<br>• Type a path for a folder or click the **Browse** button to navigate to a folder. |
| **Local View: Network Publisher Orders folder** | The Network Publisher Order Files folder is on the Rimage computer. This is the Phoenix RSM client computer's view of the export folder on the Rimage computer. The client computer refers to the computer where Phoenix RSM is running. |

© 2015

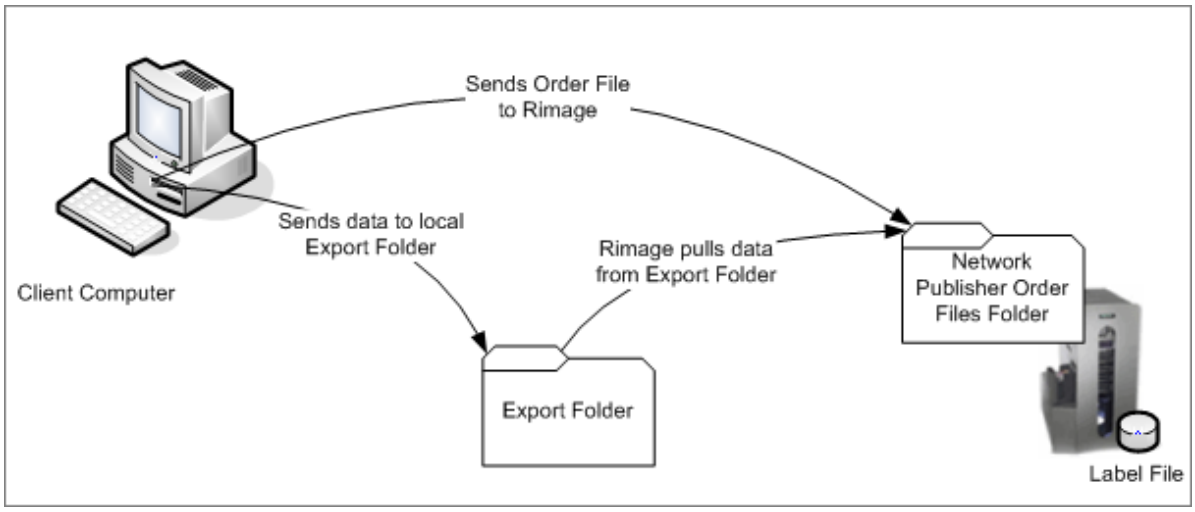
| | |
|---|---|
| | • Type a path for a folder or click the **Browse** button to navigate to a folder. |
| **Remote View: Export folder** | The view of the export folder on the Phoenix RSM client computer from the Rimage computer. This is the export folder on the client computer where Phoenix RSM is running.<br>• Type a path for a folder or click the **Browse** button to navigate to a folder. The path indicates how this folder is viewed by the Rimage system. |
| **Remote View: Disc label** | The client computer's view, where Phoenix RSM is running, of the path where Rimage gets the label file for the discs to be burned.<br> For Phoenix RSM to interact with the disc label that Rimage uses when creating discs, the disc label must already be created. |
| **User Assigned Merge fields: Number of fields** | The number of user defined fields (0 - 30). Use these fields to add label merge text to the label that is used for your media. Every field defined here is added to the Export Job Configuration pane, where you can define the contents of each field.<br> If you type a number manually, you must press TAB or ENTER for the new number to take effect.<br> Ensure that the fields entered match the fields on the disc label that Rimage uses. If the fields do not match, disc labels do not print correctly. |
| **Save configuration for all users** | Select to keep the same values for all logged-in users who use Phoenix RSM on the current computer. |

When done with the settings, click **Save**. The **Rimage** option is activated in the Export Job Configuration pane under **Export Destination**.

To export to Rimage, make sure the required Rimage system folders are in place and system permissions are set correctly.

As illustrated in the diagram below, when an Export job is executed, Phoenix RSM sends data to the Export folder on the local system and an Order file to the Network Publisher Order Files folder on the Rimage computer. Rimage takes care of the rest. In the diagram, the label file resides on the Rimage computer, but it can easily reside on any networked computer that Rimage has access and security permissions to.

© 2015




### Folder Access and Permissions Settings

To enable Rimage Export functionality, the Rimage Network Publisher must be installed and running on the network, and the Rimage Orders folder must be visible from the computer where Phoenix RSM is running. Check the following:

- There is a Rimage export folder on the Phoenix RSM client desktop computer.
- Phoenix RSM users have write access to the export folder and Rimage has at least read permissions.
- Security is set for domain users to have full control.

For more information see Export Surveillance Video.

# Data Management

SoleraTec's Phoenix RSM is the ultimate data management tool, providing automated digital asset management for Windows, Mac, and Linux environments. The Data Services Service is the engine that manages all the data within your Information Repository.

From data and video ingest or capture all the way to storage, Phoenix RSM stands out among other data management systems because your data assets are under complete control and quality is preserved. The Data Services Service delivers the peace of mind that data and video from yesterday or five years ago that is stored in the Information Repository can be searched, played back, and exported to any desktop on the network at any time.

Through creating a Data Service Policy, the Data Services Service performs duties such as migrating, replicating, and purging data between Vaults, and the overall management of data, video, and supports file movement to other Vaults on the network.

© 2015

The migration, replication, and purging of data is key to Phoenix RSM because those functions allow for a very scalable solution. Many types of storage devices may be used with Phoenix RSM and can be added as you need them. This proves to be cost effective and even more scalable for long-term retention with this multi-tiered architecture.

Since the Data Services Service manages the data between Vaults within the Information Repository, it is the Locator Service that tracks which Vaults on the network are active.

The product architecture proves advantageous with the following:

- **Load Balancing** - You can mark a specific storage pool as part of the destination criteria for jobs. The clients locate the Vault(s) that contain the designated storage pool and stores the defined files to it. If there are multiple Vaults with media belonging to the storage pool defined for the initial job, clients pick the one with the most available free space on it. This keeps the entire Information Repository load balanced.

- **Complete and Accurate Stored Files** - As a job is running, the completeness and accuracy of the stored files are constantly being verified. Most other products that perform data verification read data from the media piece and compare it to the original data on the client computer. This method is resource intensive and time consuming. Phoenix RSM uses a cyclic redundancy check (CRC) as the files are written to storage media.

If an error occurs while running jobs that prevents files from being processed, clients add the files to an internal retry list. At the end of the job, the client retries to process the files that failed on the first pass. If it fails during the retry session, the failure is logged to a retry file and report and is included in the Information Repository's error logs. When a subsequent job starts, the system looks for the retry file, and the files slated for retry are added with first priority to the list of files to be captured.

## Workflow - Data Service Policy

An intricate part of data management is working with Data Service Policies. The following steps supply an overview look at the data management workflow:

1. From your suite of product applications, open the Data Service Policy application (DataSvcPolicies.exe). For further explanation of how to launch applications using different operating systems, see Getting Started.

2. If a policy does not open by default, you need to create a policy. Before you can set parameters and initialize the process, a policy must be created and opened.

3. From the Data Service Policy window, select the Source tab to identify a Vault, media, or storage pool to migrate, replicate, or purge files.

4. From the Data Service Policy window, select the Criteria tab to designate files to migrate, replicate, or purge. Within this tab, you can also add file and directory filters.

5. From the Data Service Policy window, select the Destination tab to specify where the files are to be migrated or replicated to.

6. From the Data Service Policy window, select the Scheduling tab to define job occurrences. By default, Data Service Policies are not scheduled to run.

© 2015

7. From the Data Service Policy window, select the Advanced tab to set options such as pre-processing and post-processing commands, log output location, connection sharing, and throttling.

8. Click the **Save** icon to start the policy.

# Data Service Policies

Use Data Service Policies to create parameters for complete data lifecycle management in the Information Repository. The service provides an easy way to move, copy, and delete data while preserving data quality and making sure it is maintained on media within a storage hierarchy that continually meets performance and storage longevity requirements of each different type of data within an enterprise.

Once data is in the Information Repository, use Data Service Policies to control which files are affected during a job to migrate, replicate, or purge. The policies also control when a job starts, where files are stored, how often a job runs, when it stops, and all other aspects of the job. Initial and subsequent storage devices do not have to be of the same technology, so configurations can be built to include anything, for example, disk to tape (D2T), or disk to disk to tape (D2D2T). Other Phoenix RSM policies run on the computer where they are created, but the Data Service Policies created affects the entire Information Repository. All Data Service Policies display and can be edited in any instance of the Data Service Policy application.

Data Service Policies take on many different forms, being broad or narrow. A single Vault can contain any number of policies that can span through multiple sites.

The following three actions are all it takes for effective data management across multiple tiers of storage. Each policy created will have one of these actions assigned to it. No two policies can have the same name.

- **Migrate** - Move files or video from one Vault to another Vault. Use migrate to move data into another Vault that may have more space available, or have better performance, or move unnecessary and older data offline completely.
- **Replicate** - Copy multiple instances of stored files that can be accessed for retrieval. Use replicate to copy data into a storage device or to share the data with another network.
- **Purge** - Remove data that is no longer needed, or use as a way to keep Vaults uncluttered and clear. The policy manages the scheduled purge.

The Data Services Policies window displays all of the Data Service Policies implemented across the Information Repository on the network. Consequently, if two or more users attempt to modify a policy simultaneously, a conflict occurs and only the changes by one are saved.

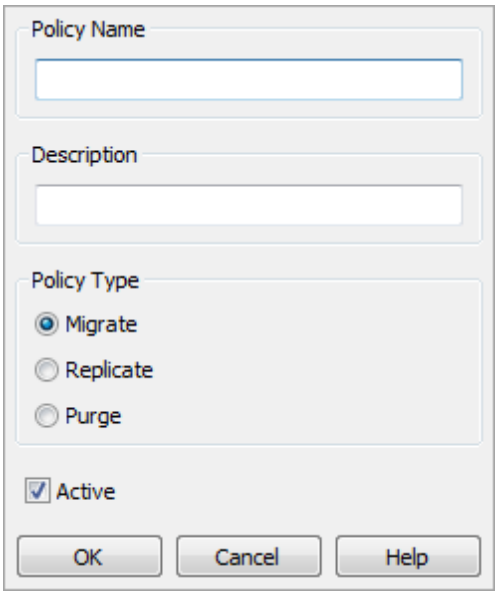
## Create a Policy

The first thing to do before working with Data Services is to create a policy. A policy has options to set for your data management needs and the policy you create determines how the Data Services Service component of Phoenix RSM manages data across your system.

© 2015

1. From your suite of product applications, open the Data Service Policies application (DataSvcPolicies.exe).

2. From the Data Service Policies window, click the plus symbol to create a new policy.




3. Type a **Policy Name** for the new policy.

4. Type a **Description** of the new policy for quick reference.

5. Select a **Policy Type**.

6. Select the policy as active, or de-select the **Active** checkbox if you do not want the policy to run. When the **Active** checkbox is de-selected, the triangular caution symbol is superimposed over the policy in the Data Service Policy window **Policy Name** pane.

7. Click **OK**. The window closes, and the policy name, description, and host appear in the **Policy Name** pane.

8. (Optional) Modify the parameters as needed on each Data Service Policy window tab for the policy. See the subsequent sections for details.

9. From the Data Service Policy window, click **Save** to keep all policy settings and implement the policy.

## Modify a Policy

Use to change a policy's name, description, and type of policy, as determined when creating a policy. Make one modification or change all controls.

1. Double-click the policy name in the Data Service Policy window **Policy Name** pane.

2. (Optional) Type a new name in the **Policy Name** text box.

© 2015

3. (Optional) Type a modified description in the **Description** text box.
4. (Optional) Select a **Policy Type**:
5. (Optional) Select the policy as active, or de-select the **Active** checkbox if you do not want the policy to run.
6. Click **OK** to accept modifications, and the window closes.
7. (Optional) Modify the parameters as needed on each Data Service Policy window tab for the policy. See the subsequent sections for details.
8. From the Data Service Policy window, click the save icon to keep all policy settings and implement the policy.

To modify a policy's parameters see the corresponding Data Service Policy window tab.

## Create a Policy and Modify a Policy Elements

| Elements | Description |
|---|---|
| **Policy Name** | The name typed here becomes the name of the new Data Service Policy. |
| **Description** | Text box to type a short description about the policy. The description should tell you something about the policy so you know what it does without having to open it. |
| **Policy Type** | Select between Migrate, Replicate, and Purge.<br>**Migrate** - Set the policy up to move files from one location to another - one Vault to another Vault. Once the data is safely moved, the original stored copy is deleted immediately.<br> When migrating from data tape media, files are marked as deleted, but are not actually deleted until the media is reused and files are overwritten. This enables migration jobs to finish in a timely manner.<br>**Replicate** - Set the policy up to copy files from one location to another - one Vault to another Vault. Retains the original stored copy.<br>**Purge** - Set policy to permanently delete files from a Vault within the Information Repository. |

© 2015

| Elements | Description |
|---|---|
| | Data Tape - When you select Purge for files on data tape media, a flag is logged in the database log index indicating deleted files. However, the files are not actually removed from the data tape until you run Erase Selected Media where media is reused and files are overwritten.<br><br>Hard Disk - Files on hard disk media are purged immediately. |
| **Active** | Select to make the policy active, and de-select to make the policy not active. If not active, a triangular caution symbol appears over the policy in the Data Service Policies window **Policy Name** pane alerting you to this condition. |

## Delete a Policy

You can delete a policy that no longer meets your needs, or you can de-activate a policy and then re-activate it at a later time if needed.

**To delete a policy:**

1. From the Data Service Policies window **Policy Name** pane, click the policy to delete.
2. Click the **Delete** button .
3. After deletion of a policy, the Data Services Service has been modified. Click the **Save** button to save the updated Data Service Policies settings.

If you delete a policy while a job is running, the job stops as soon as it is finished processing the current file.

**To make an active policy inactive:**

1. From the Data Service Policy window **Policy Name** pane, double-click the policy.
2. In the **Modify Selected Policy** window, de-select the **Active** checkbox.

## Import/Export Data Service Policies

Policy import and export functionality offered by SoleraTec's Phoenix RSM allows you to save policies, restore policies, and copy sets of policies from one computer to another. After creating a set of policies, you can export them to a policy file. Then, at a later time, if you want to re-implement the set of policies or implement them for the first time on another computer, they are there for import.

© 2015

Use the import and export functionality to take a snapshot of the working policy configuration, bring new computers online, test different policy configurations, or restore user corrupted policy configurations.

By default, recording policies are exported to **CameraPolicies.cfg**.Data service policies are exported to **DataSvcsSvc.cfg**.

Although each policy editor uses only one policy set at a time, multiple policy sets exported to policy files can be used. Create, name, and use any file naming convention for policy files, and be sure to keep track of where policies are exported to if it is a location other than the default location (the user's home directory).

Before restoring a set of policies to a computer that currently has policies set up, be sure to delete all of the current policies before importing other policies - otherwise imported policies are added to current policies.

Data Service Policies are incompatible with other client policies and vice versa. If you try to import a Data Service policy into a non-Data Service Policies client (or vice versa), an error message appears and no policies are added.

## Import Policies

When importing policies, they are added to the policies that are already in the policy editor.

1. From the application's main menu (or policy editor), click **File** > **Import from**. The Import from window appears.
2. If you are not importing policies from your local computer, navigate to the networked computer that contains the policies that you need.
3. Select the policy file that contains the policies that you want to use.
4. Click **Open**. The policies in the configuration file are implemented.

## Export Policies

1. Create policies.
2. From the application's main menu (or policy editor), click **File** > **Export to**. The Export to window appears.
3. To save your policies with the default policy file name, click **Save** without entering a new file name. Or, enter a new name In the Export to window, and then click **Save**.

## Import/Export Policy File Structure

An exported policy file is block structured but free from any column or order formatting. The tokens listed below specify job criteria. By default, policy files are exported to and imported from <install-dir>/Config/DataSvcsSvc.cfg.

© 2015

Files that contain policies are formatted as follows. Each policy is a single block. The beginning of each block is indicated by policy_name="<policy name>".

```
policy_name="<policy name>"
[
    <token>=<value>
    <token>=<value>
    . . .
]
policy_name="<policy name>"
[
    <token>=<value>
    <token>=<value>
    . . .
]
. . .
```

## Token/Value Pairs

A token is a job attribute that is given a value that determines how the job runs.

| Token/Value | Description |
|---|---|
| absolute_start = <*yyyy*>/<*mm*>/<*dd*>-<*hh*>:<*mm*>:<*ss*> | The exact start time and date that the job is to run. Multiple absolute start tokens may be entered.[1, 2] |
| active = <*boolean*> | Define if the policy is active or inactive.[2]<br>Valid values = true \| false<br>Default = true |
| complete = <*boolean*> | Print all summary information plus the path names of the files migrated to the file indicated by the list_pn option.<br>Valid values = true \| false<br>Default = false |
| content_filter = "<*character string*>" | A word or phrase in the file to be processed.<br>Default = "" |
| data_paths = <*number*> | The maximum number of concurrent files permitted to be sent during a job.<br>Default = 1 |
| deleted_files = <*boolean*> | Include files tagged for deletion.<br>Valid values = true \| false |

© 2015

| Token/Value | Description |
|---|---|
| | Default = false |
| description = "<*character string*>" | A description of the policy.[2]<br>Default = "" |
| diag = <*boolean*> | Print diagnostic information to the path indicated in the list_pn option.<br>Valid values = true \| false<br>Default = false |
| dir_spec = "<*pathname*>" | Directories to include. Multiple dir_spec options can be specified. The dir_spec check is made for every directory found. This includes the directories contained in the path name list that the job traverses.<br>Default = "*" (any) |
| display_only = <*boolean*> | Search for target files without processing them. List the files that would have been processed.<br>Valid values = true \| false<br>Default = false |
| dst_media_name = "<*character string*>" | The destination media name. If not specified, the first available unit of media is used.<br>Default = "*" (any) |
| dst_media_speed = <*character string*> | The destination media to be used according to media speed.<br>Valid values =<br>• S0 - S10<br>• Unspecified<br>Default = Unspecified |
| dst_media_type = <*character string*> | The destination media type to be used.<br>Valid Values =<br>• Hdisk - hard disk<br>• 8mm - Eight-millimeter tape |

© 2015

| Token/Value | Description |
|---|---|
| | • Dds - Digital data storage<br>• Dlt - Digital linear tape<br>• Ait - Advanced intelligent tape<br>• SuperAit - Super advanced intelligent tape<br>• Vxa - Exabyte VXA tape<br>• Travan - Travan tape<br>• Lto - Linear tape open<br>• MagOptical - Read/write optical<br>• Unspecified<br>Default = Unspecified |
| dst_storage_pool = "<*character string*>" | Specify the name of the destination storage pool to be used. Use "" for no storage pool name.<br>Default = "*" (any) |
| dst_vault_name = "<*character string*>" | Specify the destination vault to be used.<br>Default = "*" (any) |
| dst_volume_format | Internal use only. |
| dst_volume_name | Internal use only. |
| dst_volume_pack | Internal use only. |
| dt_access = <*alpha*><*yyyy*>/<*mm*>/<*dd*>-<*hh*>:<*mm*>:<*ss*> | Process files based on the accessed date and time.<br>Valid values =<br>• AO (Absolute Old) – Select files with a dtu (date_time_use) equal to or before the specified date. Enter the year as a 4-digit number.<br>• AN (Absolute New) – Select files with a dtu equal to or after the specified date. Enter the year as a 4-digit number.<br>• RO (Relative Old) – Select files with a dtu equal to or before the relative specified date. |

© 2015

| Token/Value | Description |
|---|---|
| | • RN (Relative New) – Select files with a dtu equal to or after the relative specified date.<br>• I (Inactive) – Do not use date.<br>Default = I |
| dt_stored = <*alpha*><*yyyy*>/<*mm*>/<*dd*>-<*hh*>:<*mm*>:<*ss*> | Process files based on the date and time stored on the Vault.<br>Valid values =<br>• AO (Absolute Old) – Select files with a dtu (date_time_use) equal to or before the specified date. Enter the year as a 4-digit number.<br>• AN (Absolute New) – Select files with a dtu equal to or after the specified date. Enter the year as a 4-digit number.<br>• RO (Relative Old) – Select files with a dtu equal to or before the relative specified date.<br>• RN (Relative New) – Select files with a dtu equal to or after the relative specified date.<br>• I (Inactive) – Do not use date.<br>Default = I |
| erase_media_if_unref = <*boolean*> | Erase the media when all the files on the media are marked for deletion.<br>Valid values = true \| false<br>Default = false |
| error_log = "<*pathname*>" | The path for the error log file. If you specify "/dev/tty", error messages display on the default output device. Supports token substitution.[2]<br>Default path for the configuration file = "%R/Logs/%P.err" |
| exclude_dir_spec = "<*pathname*>" | Omit directories. Accept multiple instances.<br>Default = "" (no directories excluded) |
| exclude_file_spec = "<*pathname*>" | Omit files. Accept multiple instances.<br>Default = "" (no files excluded) |

© 2015

| Token/Value | Description |
|---|---|
| file_spec = "<*pattern*>" | Files to be processed. This token/value pair can be specified multiple times to include multiple file filters.<br>Default = "*" (any) |
| hostname = "<*host name*>" | Select the files that are to be processed based on the original host name for the file.<br>Default = "" |
| include_offline = <*boolean*> | Process files from offline media.<br>Valid values = true \| false<br>Default = false |
| job_type = <*alpha*> | Specify the job type.<br>Valid values =<br>• replicate<br>• migrate<br>• purge<br>Default = migrate |
| list_pn = "<*pathname*>" | The filename where all report information is written. Supports token substitution.<br>Default path for the policy file = "%R/Logs/%P.log" |
| max_file_size = <*number*> | The maximum size in bytes of a source file. The min_file_size and max_file_size options are mutually exclusive.<br>Default = 18446744073709551615 |
| min_file_size = <*number*> | The minimum size in bytes of a source file. The max_file_size and min_file_size options are mutually exclusive.<br>Default = 0 (none) |
| out_of_band = <*boolean*> | Enable the application to constantly monitor its processes and select the network transmission protocol that best suits the files being processed.<br>Valid values = true \| false |

© 2015

| Token/Value | Description |
|---|---|
| | Default = true |
| post_proc_cmd = "<*command*>" | A command that runs immediately after the job is finished. Supports token substitution.<br>Default = "" |
| pre_proc_cmd = "<*command*>" | A pre-process command that runs immediately before a job starts. Supports token substitution.<br>Default = "" |
| process_directories = <*boolean*> | Directories will be processed.<br>Valid values = true \| false<br>Default = true |
| process_files = <boolean> | Files will be processed.<br>Valid values = true \| false<br>Default = true |
| repeat_interval = <*hh:ss:mm*> | The amount of time that elapses before a job is repeated.[1, 2]<br>Default = 24:00:00 |
| src_high_water_mark = <*number*> | The maximum percent (%) of media that is to be used. If the % used is greater than the entered value, the file is processed.<br>Valid values = 1 - 100<br>Default = 0 |
| src_low_water_mark = <*number*> | The minimum percent (%) of media used after the high watermark has been reached. If the % of media used is greater than this value and the high watermark has been reached, the file is processed.<br>Valid values = 1 - 100<br>Default = 0 |
| src_media_name = "<*character string*>" | The source media name.<br>Default = "*" (any) |
| src_media_speed = "<*character string*>" | The source media speed. |

© 2015

| Token/Value | Description |
|---|---|
| | Valid values =<br>• S0 - S10<br>• Unspecified<br>Default = Unspecified |
| src_media_type = "<*character string*>" | The source media type from where the file should be processed.<br>• Hdisk - Hard disk.<br>• 8mm - Eight-millimeter tape.<br>• Dds - Digital data storage.<br>• Dlt - Digital linear tape.<br>• Ait - Advanced intelligent tape.<br>• SuperAit - Super advanced intelligent tape.<br>• Lto - Linear tape open.<br>• Vxa - Exabyte Vxa tape.<br>• Travan - Travan tape.<br>• MagOptical - Read/write optical.<br>• NullDevice<br>• Unspecified<br>Default = Unspecified |
| src_storage_pool = "<*character string*>" | The source storage pool.<br>Default = "*" (any) |
| src_vault_name = "<*character string*>" | The source vault name.<br>Default = "*" (any) |
| src_volume_format | Internal use only. |
| src_volume_name | Internal use only. |
| src_volume_pack | Internal use only. |
| start_days = <*mtwtfss*> | The days the job is to run. Use **-** to indicate days the job should not run. |

© 2015

| Token/Value | Description |
|---|---|
| | For example, if the job is to run on Thursday, you would enter ---t---.[1, 2]<br><br>Default = mtwtfss |
| start_time = <*hh:mm:ss*> | The time the job should start for each defined start day in start_days.[1, 2]<br><br>Default = 0:0:0 (midnight) |
| stop_time = R<*yyyy*>/<*mm*><br>/<*dd*>-<*hh*>:<*mm*>:<*ss*> | The date and time the job is to stop. The date and time entered is relative to the start of the job.[2]<br><br>Default = R0000/00/00-00:00:00 (no stop time) |
| summary = <*boolean*> | Print the start and stop times and final statistics of the job to the file indicated by the list_pn option.<br><br>Valid values = true \| false<br><br>Default = true |
| throttle = <*number*> | The throttle controls the amount of bandwidth used by jobs (and, the speed files are sent to Vaults). Throttle values are relative to Information Repository capacity and range from 1% to 100%. A lower setting reduces the amount of available bandwidth that is used.<br><br>Valid values = 1 - 100<br><br>Default = 100 |
| type = <*alpha*> | The policy type of the policy file.<br><br>Default = "ds" |
| vcs = <alpha><*number*> | Specify the number of files (F) or number of bytes (S) to store per single Vault connection.<br><br>Valid values =<br>• F – files<br>• S – bytes<br>• 1 - ∞<br><br>Default = F500 |
| version = "<*number*>" | The version number of the policy. The current version number is 1.0.[2] |

© 2015

| Token/Value | Description |
|---|---|
| volume_use | Internal use only. |

[1]**Note:** Timing tokens are mutually exclusive. Only one timing token may be set. In other words, you may set either absolute_start, or repeat_interval, or start_days and start_time.

[2]**Note:** Token/Value pair is used for policy only.

## Sample Data Service Policy

If you were to export a policy, it would look similar to the following:

```
#
# Start of object rule for policy name
'Virtualization2LongTerm'
#
policy_name = "Virtualization2LongTerm"
[
    type                    = "ds"
    description             = ""
    version                 = "1.0"
    active                  = false
    complete                = false
    process_files           = true
    process_directories     = true
    content_filter          = ""
    data_paths              = 1
    deleted_files           = false
    diag                    = false
    display_only            = false
    dst_vault_name          = "*"
    dst_media_name          = "*"
    dst_storage_pool        = "LongTerm"
    dst_media_speed         = Unspecified
    dst_media_type          = Unspecified
    dst_volume_format       = Unspecified
    dst_volume_name         = "*"
    dst_volume_pack         = ""
    dt_access               = I
    dt_stored               = I
    error_log               = "%R/Logs/%P.err"
    hostname                = ""
    include_offline         = false
    job_type                = "migrate"
    list_pn                 = "%R/Logs/%P.log"
    min_file_size           = 0
    max_file_size           = 18446744073709551615
    src_vault_name          = "*"
    src_media_name          = "*"
```

© 2015

```
      src_storage_pool          = "Virtualization"
      src_media_speed           = Unspecified
      src_media_type            = Unspecified
      src_volume_format         = Unspecified
      src_volume_name           = "*"
      src_volume_pack           = ""
      volume_use                = Unspecified
      out_of_band               = true
      post_proc_cmd             = ""
      pre_proc_cmd              = ""
      repeat_interval           = 00:00:20
      src_high_water_mark       = 80
      src_low_water_mark        = 80
      stop_time                 = R0000/00/00-00:00:00
      summary                   = true
      throttle                  = 100
      vcs                       = F500
  ]
```

## Data Service Policies Window

The Data Service Policies window is divided into two main panes. The left pane provides an overview of all of the Data Service Policies in the Information Repository noting the policy name, type and description. The right pane consists of the Source, Criteria, Destination, Scheduling, and Advanced tabs to populate when creating a policy.

Use the Data Service Policies toolbar to create a new policy by clicking the **Add** button. The toolbar consists of the following buttons:

- Save all policy settings.

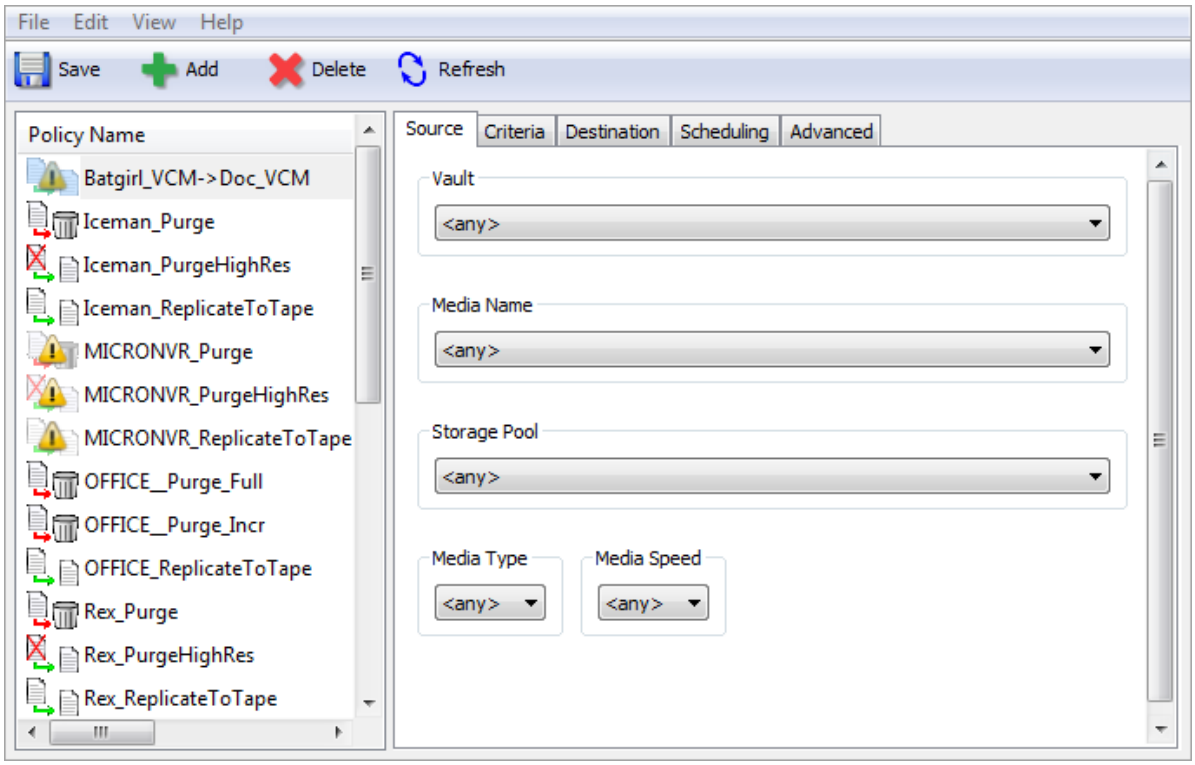
- Add a new policy.

- Delete the selected policy.

- Refresh the view for the latest version of each policy to display. Since Data Service Policies are implemented across the whole Information Repository, refreshing is important to do to get the latest updates for the Data Service Policies view. Also, it refreshes for changes that could affect contents of Vaults, media names, and storage pools. Before you refresh, save. If you do not save, any changes made or added policies will be lost.

The Data Service Policies window is described below:

© 2015




The triangular caution symbol on the policy icon in the left pane of the window indicates that the policy is not active.

## Data Service Policy Menu Items

| Menu Items | Description |
|---|---|
| **File > Save All Policy Settings** | Save settings for policies created or modified. |
| **File > Import from** | Open an Import from window to select a Data Services Service configuration file that contains values for a policy. |
| **File > Export to** | Open an Export to window to select where a Data Services Service configuration file saves to. |
| **File > Exit** | Close the application. If changes have been made a Confirmation dialog box appears for saving changes, click **Yes**, **No**, or **Cancel**. |
| **Edit > Create a Policy** | Open the Create a Policy window. Assign a new policy name, description of policy, and the type of policy. Also indicate if you want the policy to be active or not. |

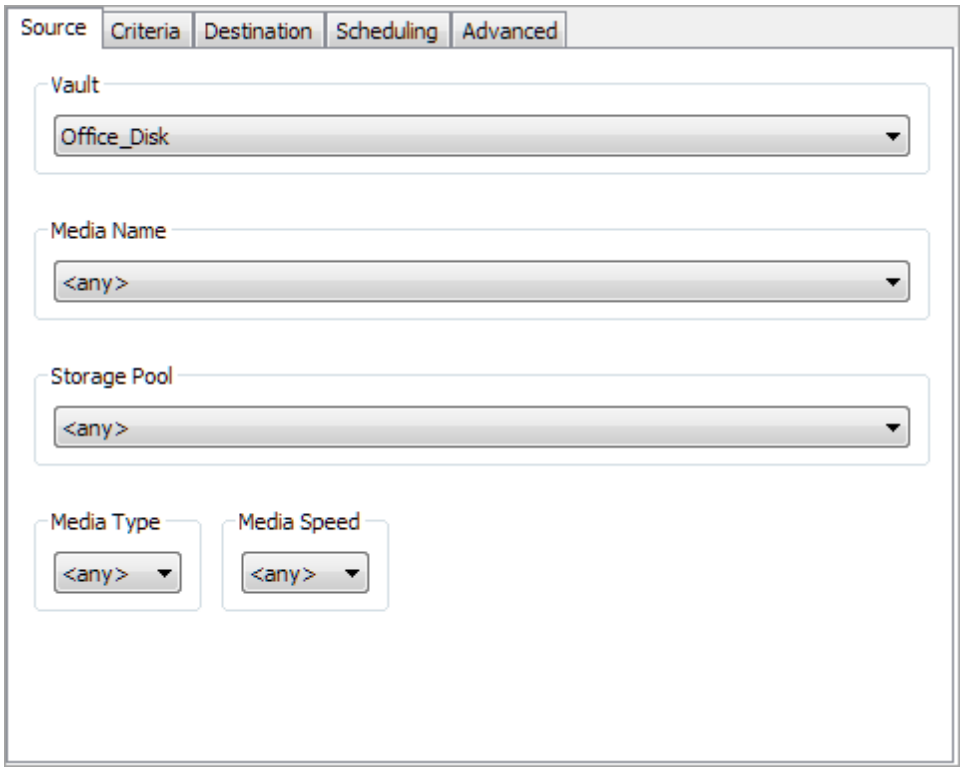
© 2015

| Menu Items | Description |
|---|---|
| **Edit > Modify Selected Policy** | Select a policy listed in the left pane, then select this menu item to modify the existing policy. |
| **Edit > Delete Selected Policy** | Select a policy listed in the left pane, then select this menu item to remove the policy from Data Services. |
| **Edit > Delete All Policies** | Delete all the policies from the configuration file, and removes policies listed in the left pane. |
| **View > Refresh Policy View** | Refresh the view in the left pane for the latest list of policies. |
| **View > Enable Tool Tips** | Check mark by this menu item indicates that tool tips for the window will display. The tips are brief descriptions of window controls if the mouse pointer is moved over a control. De-select to turn tool tips off. |
| **View > Enable Policy Tips** | Check mark by this menu item indicates that policy tips display in the left pane. Policy tips provide details of the policy as set using the right pane tabs. De-select to turn policy tips off. |
| **Help > Current Page** | Open online help to the Data Services Policies webpage. |
| **Help > Data Service Policies Overview** | Open online help with focus on Data Services Policies. |
| **Help > Contents** | Open the local version of online help. |
| **Help > Online Help** | Open the web-based version of online help. |
| **Help > Online Support** | Open the support webpage. |
| **Help > About Data Services Policies** | Open the About Data Services Policies window. |

## Data Service Policies Source Tab

After a Data Service Policy has been added, the next step is to define the source where files are migrated, replicated, or purged from. Use the **Source** tab to specify parameters for the policy for where files come from. The point of origin can be a Vault, media, storage pool, media type, or media speed.

© 2015




The drop-down elements include a default setting of <any>. If you leave the default setting, then all information from all sources is processed for the given field. For example, if the Vault drop-down is set to <any>, then data from all Vaults within your Information Repository is processed.

Adding to that, the parameters of <any>, <unnamed>, and <new entry> are not placeholders, they are actual names used in your Information Repository - unless changed to alternate names.

Unless you have added new names, only <any>, <unnamed>, <new entry>, and names of Vaults, media, storage pools, media types, and media speeds already implemented in the Information Repository appear in the drop-down lists.

If you plan to add new Vaults, media, or storage pools to the Information Repository and already know names to assign, you can add them manually. However, it is best to select only media that appears in the drop-down list. There are several options for doing this:

- **Leave defaults (<any> or <unnamed>) and use the Criteria tab to define data to be processed** - Phoenix RSM selects the most accessible Vault and media with the most free space.
- **Select a value from a Source tab group that contains data to process** - Phoenix RSM processes data only from the drop-down list where a value has been selected. For example, if Media Speed S8 is selected, only media with an S8 speed rating is processed. If only a Vault is selected, then data is processed only from the selected Vault, including all of the media and storage pools within the Vault.
- **Select values from every Source tab group for a more focused process** - If values for Vault, Media Name, and Storage Pool have been selected, the options available in the remaining fields are limited according to values already set. For instance, a single storage pool may only contain a few media types to choose from.

© 2015

- **Create a new entry for Vault, Media Name, or Storage Pool** - Select from the drop-down list <new entry>. A window appears to type a new name. Click **OK**, and the new entry appears in the drop-down list.

  This new name is a placeholder. A Vault cannot be used until it has been added using the Add and Remove Vault Wizard, and the media and storage pool have to be configured using the Vault Admin's Prepare Media window. If you try to run a job without configuration, the job will fail. Drop-down list names above <any> are running in the Information Repository. The names below <any> have not yet been configured.

To reset the **Source** tab, select **<any>** from the Vault drop-down list.

## Data Service Policy Source Tab Elements

| Element | Description |
|---|---|
| **Vault** | From the drop-down list select a Vault, or select **<new entry>** to add a new Vault name.<br><br>If a Vault is selected, the Media Name drop-down is automatically populated with the media on the given Vault.<br><br>If a new entry is given, then the Media Name and Storage Pool options are limited to <any> or <unnamed> and <new entry>. |
| **Media Name** | Media Name refers to the names of individual units of media in the Vaults within the Information Repository.<br><br>From the drop-down list select the media, or select **<new entry>** to add a new media name. The system automatically looks for any storage pools comprised of the selected media. If it cannot find any, then the Storage Pool drop-down list displays <any>. |
| **Storage Pool** | Storage pools are groupings of media on a single policy used for a particular purpose. For example, if you had a policy called "Night backup" and it wrote to several units of media, you would use a "Night backup" storage pool and assign to it every unit of media to use for that purpose. For more information see Prepare Media, Storage Pool.<br><br>From the drop-down list select a storage pool, or select **<new entry>** to add a new storage pool name. |
| **Media Type** | Determine the types of media a policy uses by specifying a media type. For example, if "Hdisk" is selected, then only Hdisk media is used. Media Type is useful for processing data of lower importance or less rigorous recovery time objectives. |

© 2015

| Element | Description |
|---|---|
| | From the drop-down list select the media type. Only media types for the parameters selected in the Vault, Media Name, or Storage Pool drop-down lists are displayed. If none were selected, then only the media types from media available within the Information Repository are displayed.<br><br>Set either Media Type or Media Speed, but not both. |
| **Media Speed** | Source files run based on speed and media performance. This is useful for processing data of lower importance or less rigorous recovery time objectives.<br><br>Hard disk is considered a high performance media and is assigned a high rating of (S8). Slower data tape technologies are lower performance and are assigned a lower rating of (S0).<br><br>From the drop-down list select a performance rating. Only media speeds for the parameters selected in the Vault, Media Name, or Storage Pool drop-down lists are displayed. If none were selected, then only the media speeds from media available within the Information Repository are displayed.<br><br>Set either Media Type or Media Speed, but not both. |

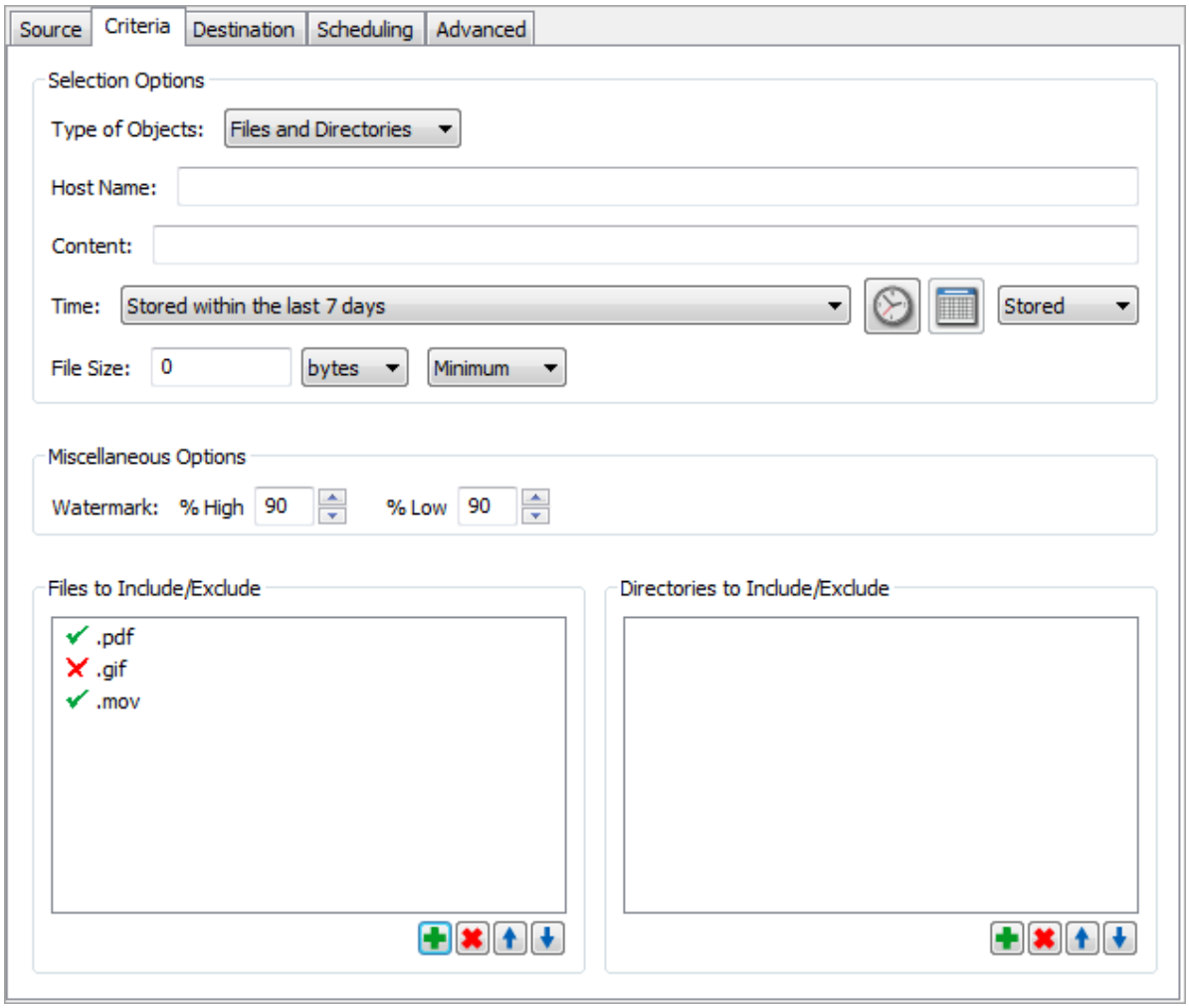
### New Entry window

If you select **<new entry>** a window appears to type a new entry for either the Vault, Media Name, or Storage Pool source. In these new entry windows you can use wildcards to better manage and specify where files are coming from. Wildcards for file filters operate on file names; directory filters operate on directory name. For more information see Wildcards.

## Data Service Policies Criteria Tab

Use the Data Service Policy **Criteria** tab after the **Source** tab. In the **Criteria** tab you can further refine which files are moved, copied, or deleted by configuring the criteria parameters. If all the fields are left empty on this tab, then all of the files that live at the source are migrated, replicated, or purged. To select files from specific locations or of specific types, use file and directory filters.

© 2015




## Data Service Policy Criteria Tab Elements

| Element | Description |
|---|---|
| **Type of Objects** | Select the types of objects for processing.<br><br>**Files and Directories** - Both files and directories are processed and rights for both are preserved.<br><br>**Files Only** - Only files and their rights are preserved, while directories are ignored.<br><br>**Directories Only** - Directories and their rights are processed, while files are ignored. |
| **Host Name** | Use this parameter to migrate all files from a particular host. The policy processes only files that originally came from the host computer named. |

© 2015

| Element | Description |
|---|---|
| | Type the name of the computer on the network to define as the host. |
| **Content** | Use to limit files processed to those containing a particular word or phrase. Be certain to enclose the phrase in quotation marks, otherwise all files containing any word typed is processed in the query. For more information see Wildcards - content searching.<br><br>Type a word or phrase to use for criteria for processing. |
| **Time** | Select files based on time and date that they were stored or on when they were last accessed.<br><br>**Time and date** process -<br><br>1. From the **Time** drop-down list, select an option that includes a specific time and date (for example, Created after HH:MM:AM on Day). The **Clock** button, **Calendar** button, and the **Created/Stored** drop-down list are activated.<br><br>2. Select **Created** or **Stored**. The text in the **Time** drop-down list changes accordingly.<br><br>3. Click the **Clock** button to select a time from the Time window. The selected time displays in the **Time** drop-down list.<br><br>4. Click the **Calendar** button to select a date from the Date window. The selected date displays in the **Time** drop-down list.<br><br>**Last accessed** process -<br><br>1. From the **Time** drop-down list, select an option that includes an interval of time (for example, Created more than x days ago). The **Clock** button and the **Created/Stored** drop-down list are activated.<br><br>2. Select **Created** or **Stored**. The text in the **Time** drop-down list changes accordingly.<br><br>3. Click the **Clock** button to determine a period of time of years, months, days, hours, and minutes from the Period of Time window. The selected period of time displays in the **Time** drop-down list. |
| **File Size** | Use to specify a minimum or maximum file size associated with the policy. This is useful for refining your file selection criteria further. |

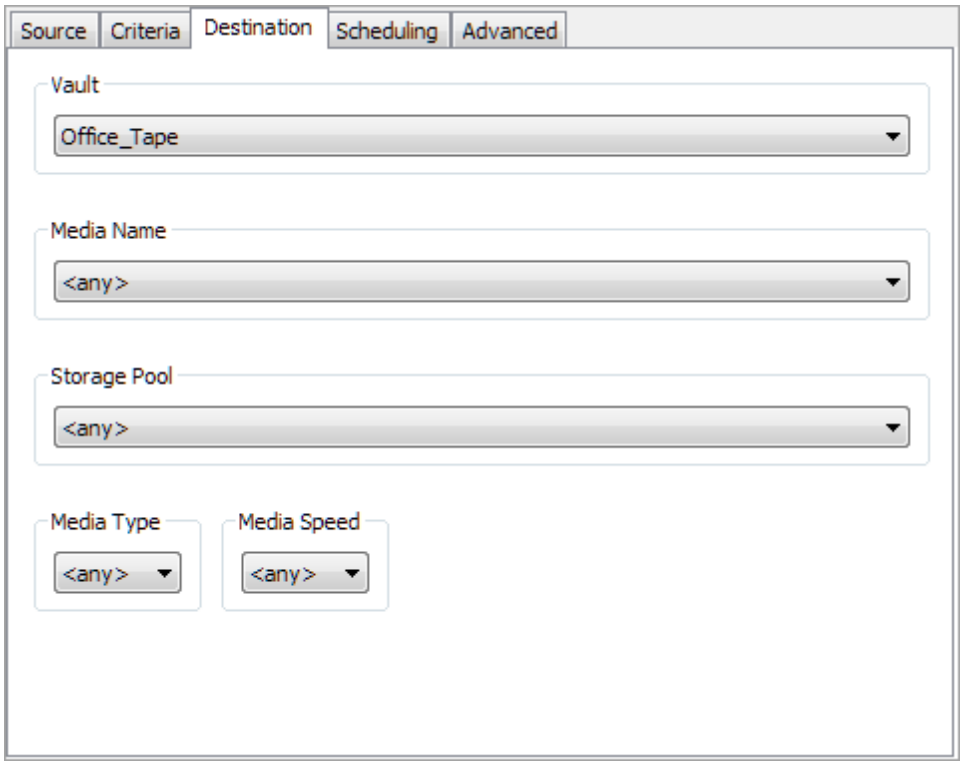
© 2015

| Element | Description |
|---|---|
| | 1. Type a file size in the text box.<br>2. Select the unit of measurement (bytes, KB, MB, GB).<br>3. Select **Minimum** or **Maximum**.<br>**Minimum** - The policy only processes files that are larger than the size specified.<br>**Maximum** - The policy only processes files that are smaller than the size specified. |
| **Watermark** | Watermarks determine when data is processed as a policy runs - in relation to the percentage of available space on source media.<br>Select a **High** watermark percentage, the processing begins when a policy runs and the amount of data on the source media exceeds the high watermark. Data processing continues until the source media reaches the level indicated by the Low watermark.<br>Select a **Low** watermark percentage, the processing stops when the amount of data on the source media reaches the low watermark. |
| **Files and Directories to Include/Exclude** | After making general selections of files and directories to process from the options above, you can apply filters to refine which files or directories to process.<br>**Include** filters - Include only specific files or directories in a job.<br>**Exclude** filters - Rule out specific files or directories from a job.<br>For more information see Filters. |

## Data Service Policies Destination Tab

Use the Data Service Policy **Destination** tab after defining the policy criteria. In the **Destination** tab you can determine the Vaults, media, and storage pools to store your data.

© 2015




Only the default names of <any>, <unnamed>, <new entry>, or implemented names of Vaults, storage pools, media, media types, and media speeds already in the Information Repository appear in the **Destination** tab drop-down lists. New names with associated parameters appear also, once added.

You can enter names of new Vaults, media, or storage pools to the Information Repository before actually adding them and the names will appear beneath <any> in the given field. However, it is recommended to select only media that appears in the drop-down list, otherwise you may increase chances of error.

There are several options for populating the **Destination** tab fields:

- **Leave the default values (<any>)** - Phoenix RSM determines the most accessible Vault and the media with the most free space.
- **Select a parameter and let Phoenix RSM take care of the rest** - For example, if the Media Speed of S8 is selected, then only media running at the speed associated with S8 writes. Or, if Storage Pool or Media Name is selected, then files are only sent to the storage pool or media selected. With a selected Vault, Phoenix RSM uses the most available Vault or media with the most free space.
- **Select a parameter and select available parameters from remaining fields** - If a Vault, Media Name, or Storage Pool parameter is selected, then remaining fields have limited options available which correspond to the parameter.

To reset the **Destination** tab with all parameters from any field, select **<any>** in the **Vault** group.

Several units of media can be assigned to a single storage pool. See Prepare Media - Storage Pool.

© 2015

- **Create a new entry for a Vault, Media Name, or Storage Pool** - From the Vault, Media Name, or Storage Pool drop-down list, select **<new entry>**. The Enter New Name window appears for you to type a new name. Click **OK** and the new entry appears in the field's drop-down list.

This method is recommended only for special circumstances. If a job is run with a Vault or media that is not actually running in the Information Repository, the job fails.

The <any> item in the drop-down list also acts as a divider between Vault, media, and storage pools implemented and those not implemented. Names above <any> are the ones running in your Information Repository, and the names below <any> are entered but do not yet have hardware implemented in the Information Repository. These are not saved if not selected when saving the policy.

The limitations to adding a new name for a Vault, Media Name, or Storage Pool are:

- Typing a new name for the Vault, Media Name and Storage Pool options are limited to <any> and <new entry>.
- New entries in Media Name or Storage Pool do not limit options in the remaining fields.
- Wildcard additions (for example, Ac*), appear beneath <any>. See Wildcards.

## Data Service Policy Destination Tab Elements

| Element | Description |
|---|---|
| **Vault** | From the drop-down list select a Vault, or select **<new entry>** to add a new Vault name.<br><br>If a Vault is selected, the Media Name drop-down is automatically populated with the media on the given Vault.<br><br>If a new entry is given, then the Media Name and Storage Pool options are limited to <any> or <unnamed> and <new entry>. |
| **Media Name** | Media Name refers to the names of individual units of media in the Vaults within the Information Repository.<br><br>From the drop-down list select the media, or select **<new entry>** to add a new media name. The system automatically looks for any storage pools comprised of the selected media. If it cannot find any, then the Storage Pool drop-down list displays <any>. |
| **Storage Pool** | Storage pools are groupings of media on a single policy used for a particular purpose. For example, if you had a policy called "Night backup" and it wrote to several units of media, you would use a "Night backup" storage pool and assign to it every unit of media to use for that purpose. For more information see Prepare Media, Storage Pool. |

© 2015

| Element | Description |
|---|---|
| | From the drop-down list select a storage pool, or select **<new entry>** to add a new storage pool name. |
| **Media Type** | Determine the types of media a policy uses by specifying a media type. For example, if "Hdisk" is selected, then only Hdisk media is used. Media Type is useful for processing data of lower importance or less rigorous recovery time objectives.<br><br>From the drop-down list select the media type. Only media types for the parameters selected in the Vault, Media Name, or Storage Pool drop-down lists are displayed. If none were selected, then only the media types from media available within the Information Repository are displayed.<br><br>Set either Media Type or Media Speed, but not both. |
| **Media Speed** | Source files run based on speed and media performance. This is useful for processing data of lower importance or less rigorous recovery time objectives.<br><br>Hard disk is considered a high performance media and is assigned a high rating of (S8). Slower data tape technologies are lower performance and are assigned a lower rating of (S0).<br><br>From the drop-down list select a performance rating. Only media speeds for the parameters selected in the Vault, Media Name, or Storage Pool drop-down lists are displayed. If none were selected, then only the media speeds from media available within the Information Repository are displayed.<br><br>Set either Media Type or Media Speed, but not both. |

## Data Service Policies Scheduling Tab

Use the Data Service Policies **Scheduling** tab to define when jobs are to run. Jobs can be scheduled to run on a daily or weekly basis while setting only a few general parameters or jobs can be scheduled using exact dates and times with specific parameters set.

A scheduled job is implemented as soon as the Data Service Policy is saved (assuming all other parameters are acceptable).

### Scheduling a Job

The Scheduling tab displays different fields to populate depending on the parameter set for the **When should the job run?** option.

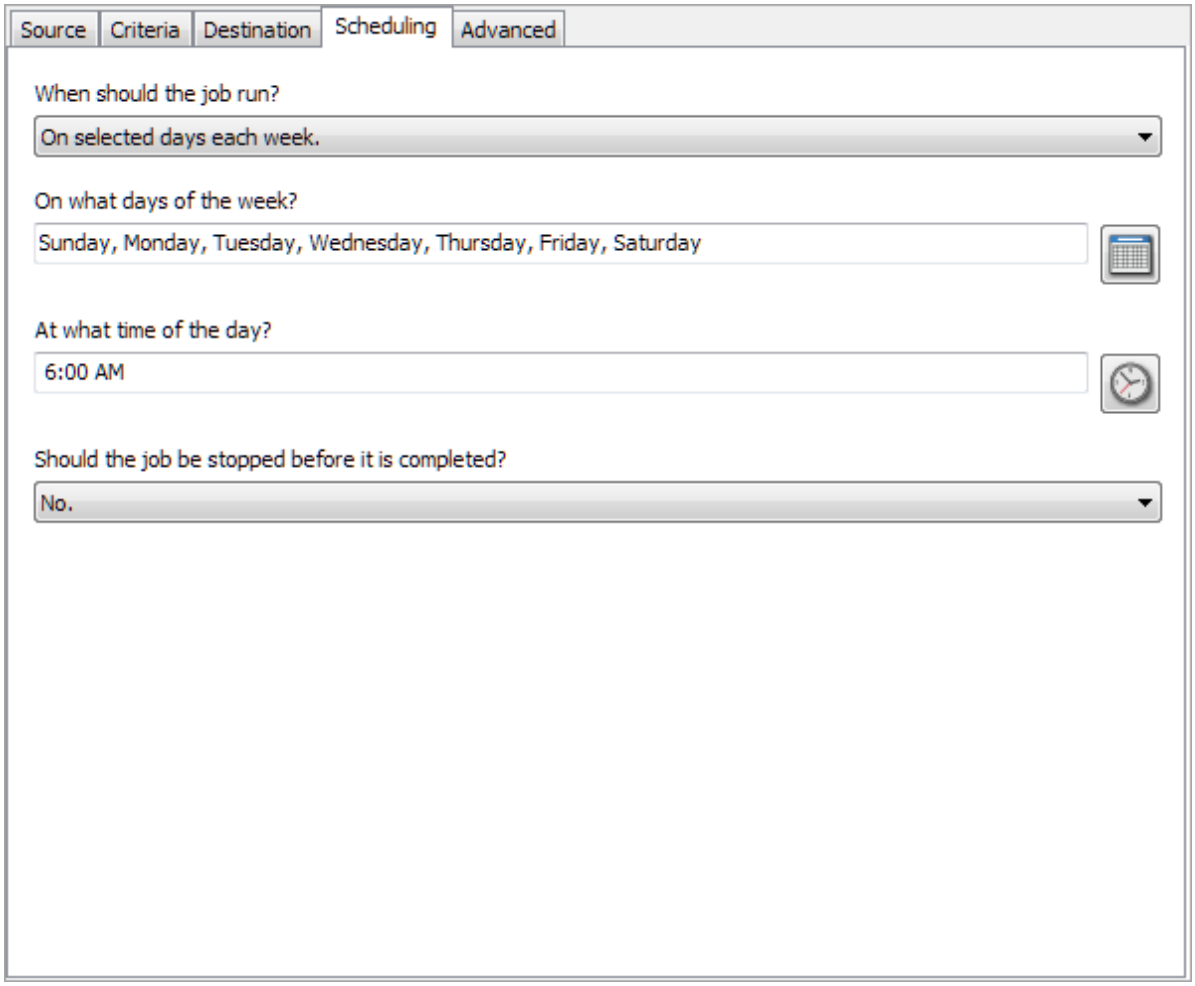
© 2015

From the **When should the job run?** drop-down list, select one of the options to schedule a process. Each are described below.

- Option 1: On selected days each week
- Option 2: Repeatedly at a defined interval
- Option 3: On specific dates & times

### On selected days each week

Use this option to schedule jobs to run on particular days at specific times. When this option is selected, the **Scheduling** tab displays as follows:




1. Next to the **On what days of the week?** text box, click the **Calendar** button to open the Days window. Set the days of the week to run the job.
2. Next to the **At what time of the day?** text box, click the **Clock** button to open the Time window. Set the time for the job to start running.

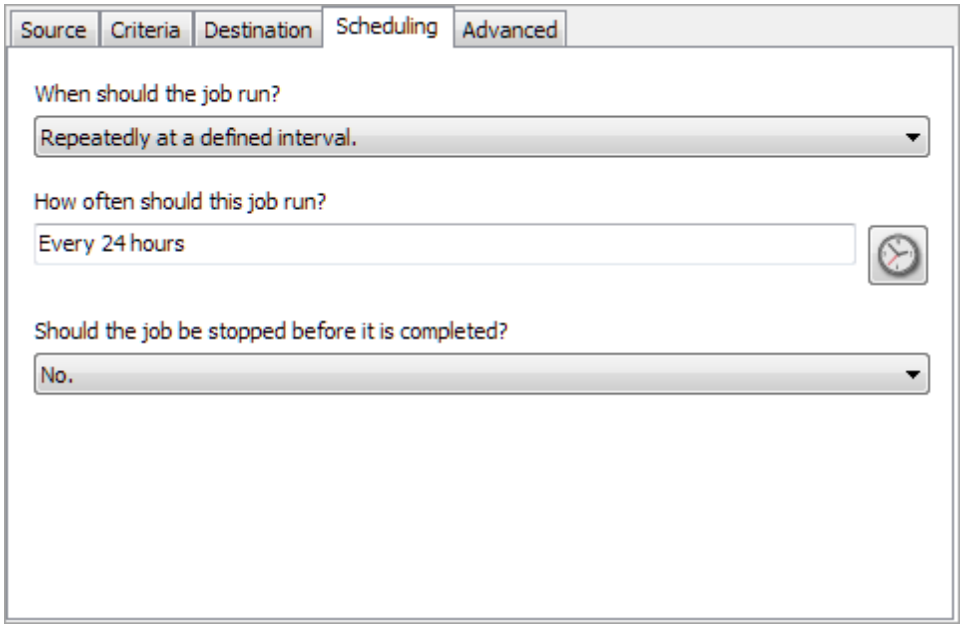
© 2015

3. Determine if the job should be stopped before it completes. This option is useful if there is or could be a conflict with another process. If **Yes** is selected, the Duration window appears for you to specify the job duration time.

For more information about the Days, Time, and Duration windows see Job Scheduling.

### Repeatedly at a defined interval

Use this option to schedule jobs to run repeatedly at a set interval, for as long as the policy is active. To stop a policy that has been set to run repeatedly, you must deactivate, change, or delete the policy. When this option is selected, the **Scheduling** tab displays as follows:



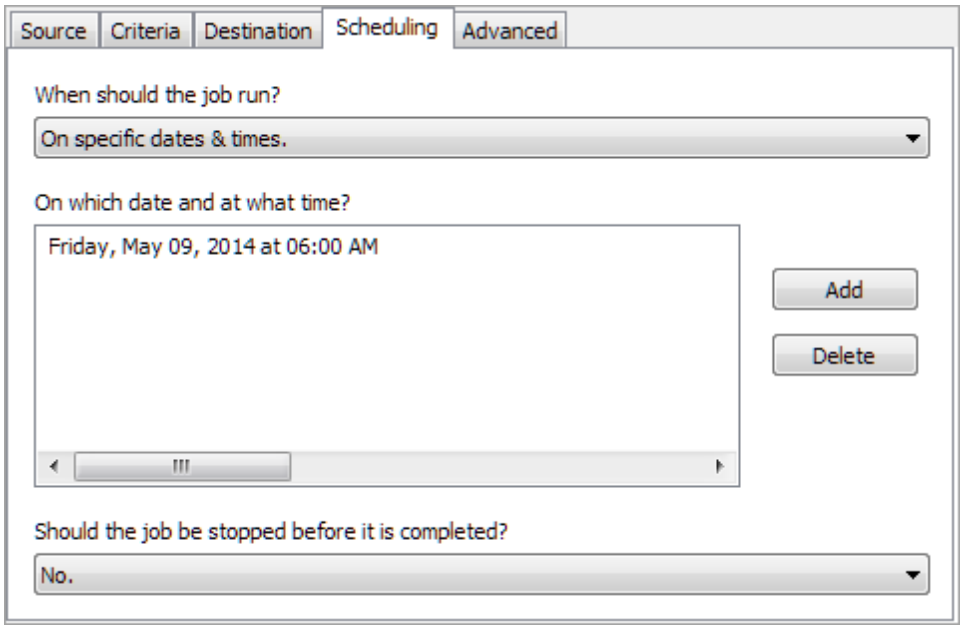

1. Next to the **How often should this job run?** text box, click the **Clock** button to open the Time Interval window. Set the interval time for the job to incrementally run.

2. Determine if the job should be stopped before it completes. This option is useful if there is or could be a conflict with another process. If **Yes** is selected, the Duration window appears for you to specify the job duration time.

### On specific dates & times

Use this option to schedule jobs to run on specific dates and times. When this option is selected, the **Scheduling** tab displays as follows:

© 2015




1. Click the **Add** button to add a scheduled runtime for the job. The Date window appears for you to select a date, and then the Time window appears for you to select a time.

2. To delete scheduled run dates and times, from the **On which date and at what time?** box, select a date and time entry and then click the **Delete** button to remove the setting.

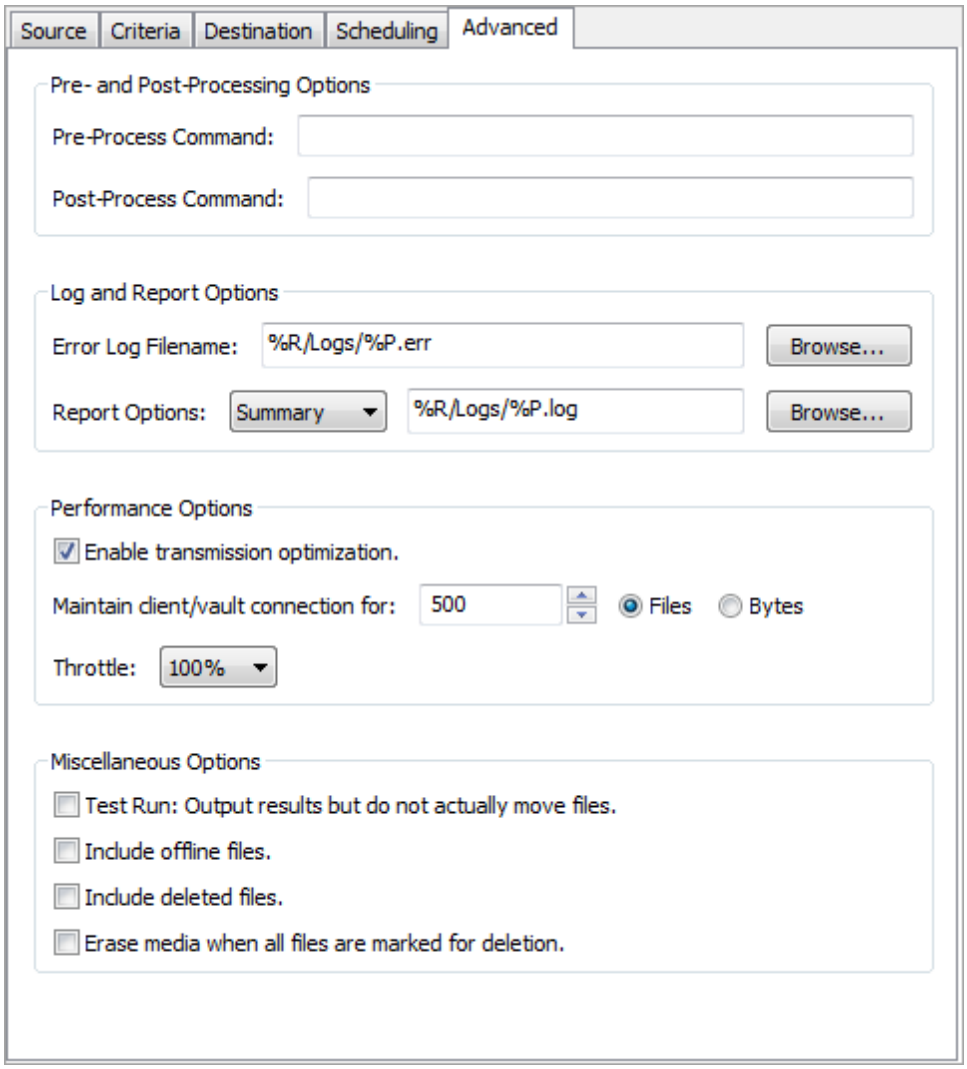
3. To edit a date and time entry, delete the entry you want to change and then add a new run date and time.

4. Determine if the job should be stopped before it completes. This option is useful if there is or could be a conflict with another process. If **Yes** is selected, the Duration window appears for you to specify the job duration time.

© 2015

## Data Service Policies Advanced Tab

Use the Data Service Policy **Advanced** tab after you have defined a schedule for your policy. The **Advanced** tab offers more options to define how your jobs operate and process.




### Data Service Policy Advanced Tab Elements

| Element | Description |
|---|---|
| **Pre- & Post-Processing Command** | Use the pre-processing and post-processing commands to execute commands before and after each session.<br><br>Type a pre-processing or post-processing command, or both, into the text boxes. Command strings can be pointers to executable files with arguments, pointers to shell scripts, or a command string that the local processor is equipped to accept. |

© 2015

| Element | Description |
|---|---|
| | The following are variables in pre-processing and post-processing commands:<br>%P or %Pn - Policy Name<br>%H or %Hn - Host Name<br>%D - Date (yyy:mm:dd)<br>%Dy - Year<br>%Dm - Month<br>%Dd - Day<br>%T - Time (hh:mm)<br>%Th - Hour<br>%Tm - Minute<br>%Ts - Second<br>%R or %Rn - Root path name. Valid only at the beginning of a string<br>%Ne - Number of errors<br>%Nr - Number of retries<br>%Nb - Number of bytes written<br>%Nf - Number for files written |
| **Error Log Filename** | An error log file is created anytime an error is encountered during a job. It is useful for troubleshooting problems. The **Error Log Filename** text box can include literal file names or a combination of file name field variables to generate file names for logs.<br>• Leave the default variables in place, or type in a file name and extension to use, or type in a variable name using file name field variables (see File Name Field Variables section below).<br>• Use the **Browse** button to define a new location and type in the file name that you want to use, including an extension. |
| **Report Options** | When a job runs, one of the following report files is created:<br>**Summary** - A header and summary report |

© 2015

| Element | Description |
|---|---|
| | **Complete** - Same as summary and lists all files<br><br>**Diagnostic** - Complete, but adds relevant, diagnostic information<br><br>• From the drop-down list select a report option. Use the **Summary** or **Complete** options on a normal basis and switch to **Diagnostics** if problems occur.<br><br>• In the **Report Options** text box, leave the default variables in place, or type in the file name and extension to use, or type a variable name using file name field variables (see File Name Field Variables section below).<br><br>• Use the **Browse** button to locate a file to overwrite an already existing log file. |
| **Enable Transmission Optimization** | Select for the client to constantly monitor its processes and to determine the best network transmission protocol for files being processed. Leave this option selected to get up to a 20% increase in performance. If the Information Repository is slow, run a few timed tests to determine a setting that works best for your Information Repository. |
| **Maintain Client/Vault Connection** | Vault connection sharing determines how many files are sent from the source Vault to the destination Vault in a single connection. The higher the number of files or bytes transferred, the longer the connection between the source and destination Vault are maintained. Access to a particular Vault resource (such as one drive of a multi-drive storage device) used by a process on one client is restricted and inaccessible to other clients in the network for the duration of the connection.<br><br>To illustrate this, imagine an environment where a single Vault with a single tape drive is used to service several desktop clients. When a client is configured with a connection sharing set to 250 files, and other clients are configured to start jobs at the same time, no client can connect until the first client is finished. Each connection to the server locks out other connections, and other clients must wait before processing files.<br><br>1. Type a value into the **Maintain Client/Vault Connection for** text box. |

© 2015

| Element | Description |
|---|---|
| | 2. Select the **Files** radio button or **Bytes** radio button. By selecting Files, a connection sharing proceeds based on the number of files transmitted; and if Bytes, based on the number of bytes. |
| **Throttle** | The throttle controls the speed that files are sent to the Vault. Lower numbers reduce the bandwidth. Throttle values range from 10% to 100% of total available bandwidth.<br>• From the **Throttle** drop-down list, select a percentage to operate the client on its host computer for maximum performance.<br>Phoenix RSM is designed to operate at maximum performance of its host computer, network environment, and storage resources available. During normal working hours, running a job at peak performance could interfere with other network operations. |
| **Test Run: Output Results but do not actually move files** | Use to test a job before doing it live. This is useful after creating a complex set of process parameters that include filters and other options.<br>• Select **Test Run: Output results but do not actually move files**. When the process is scheduled to run, the files that match the criteria build, but files are not moved. Results output in a report, defined in the **Report Options** field. |
| **Include Offline Files** | Since all of your stored files are logged, you can include offline files when processing jobs. If the files are located on offline media, the job requires more time as the system has to wait whenever offline media is required. |
| **Include Deleted Files** | Process files marked as deleted in tape media.<br>• Select to set the policy to process files marked as deleted. If this option is de-selected the policy ignores these files.<br>On media types, like magnetic tape, it is not possible to remove files that have been deleted or purged from the Information Repository. Because it writes sequentially, a file marked for deletion may lie on the media between two viable files. The files eligible for removal are marked as deleted even though they remain on the media. |
| **Erase media when all files are deleted or no longer referenced** | Media will be erased when all the files stored on that media have been marked for deletion. |

© 2015

| Element | Description |
| --- | --- |
| | • Select this option to erase the media when all files are deleted or no longer referenced.<br><br>For media which do not support random file deletion (i.e. tape), this will make the media fully available and usable again.<br><br> This option is only enabled when a policy is a **purge** or **migrate** policy. |

© 2015

### Offline Media

During a data service job, offline media is used only if **Include offline files** is selected from the **Advanced** tab. If **Include offline files** is not selected, attempting to use media that is offline may result in a "No resources available" error if media cannot be found.

### File Name Field Variables

The file path can include a literal file name or a combination of variables to generate file names for reports. Use variables to distinguish between reports and to find specific reports.

If a path with a literal file name is typed like C:/Program Files/Logs/Job_Report.log, the system generates the report destination folder Logs (if it does not already exist) and a report named Job_Report.log. If a path with variables for the file name is typed, for example, %R/Logs/%P_from_%H_on_%D_at_%T, the system generates the report destination folder and a report — where policy name, host name, date, and time are populated with the actual details from your Information Repository and job.

The following are the variables to use. When using multiple variables, separate them from each other with an underscore (_).

| Variable | Description |
|---|---|
| %P or %Pn | Policy Name |
| %H or %Hn | Host Name |
| %D | Date (yyyy:mm:dd) |
| %Dy | Year |
| %Dm | Month |
| %Dd | Day |
| %T | Time (hh:mm) |
| %Th | Hour |
| %Tm | Minute |
| %Ts | Second |
| %R or %Rn | Root Pathname. Valid only at the beginning of a string |

# Customization

SoleraTec's Phoenix RSM has many strengths for managing your digital data assets. One of the key benefits is the ability to customize Phoenix RSM and really make it your own so that it is the best solution it can be for your specific needs.

© 2015

The customization topics are intended for advanced users and are easy to use once mastered. Phoenix RSM applications are highly customizable through use of the following items:

- **Wildcards** - Phoenix RSM supports the use of wildcards for more efficient data asset searches.
- **Filters** - Make use of filters during data asset searches, with or without wildcards, to include or exclude specific (or groups) of files or directories.
- **ExportExtensions.cfg** - Use to customize export options for files and video that have been retrieved.
- **Site.cfg** - Use to work remotely on a network subnet that does not have multicast capabilities.
- **Command line arguments** - Use as an alternative way for executing functionality for Phoenix RSM applications.
- **Key configurations** - Use to modify default functionality settings as seen in the application interfaces.

# Wildcards

For effective, thorough, and quick searching, Phoenix RSM offers the availability of employing wildcard characters throughout all applications. Wildcards are useful for searching and filtering stored video, files and file names, directories and directory names, and content within your Information Repository. See also Filters .

The two types of wildcards Phoenix RSM recognizes are:

- **POSIX standard wildcards** - For use in path names, filtering, and metadata searching.
- **Regular expressions** - For use only in text or content searching. For example, a word in a file.

## POSIX Standard Wildcards

Use these standard wildcards when creating file and directory filters or when searching for files and metadata. These wildcards are convenient to use in text boxes on windows dealing with the Vault, Media Name, and Storage Pools. Wildcards for file filters operate on file names; directory filters operate on directory name.

A single wildcard character represents a single variable in a query and wildcard operators search for words with variable characters.

The following are things to keep in mind when using the standard wildcards:

- Wildcards can be used in combination with other wildcard characters.
- Searches are not case sensitive.
- These wildcard operators do not work for content searching (you must use the regular expressions).
- For predictable results when using wildcards for metadata, it is best to avoid using * and #.

© 2015

## POSIX Standard Wildcard Table

The table below lists all the wildcard operators for conducting file, metadata, and window text box searches. Two basic and common operators (they are the first two in the table), are highlighted for quick query reference:

**? = a single character wildcard, to represent a single variable.**

*** = a string wildcard, to represent a variable string of zero or more characters.**

| Wildcard | Description |
|---|---|
| **?**<br><br>**Any single character** | Substitutes a single character or can be combined to represent multiple characters. Use the ? for specific alternative spellings.<br><br>? substitutes a single character<br><br>?? substitutes two characters<br><br>??? substitutes three characters, and so on.<br><br>If used in a path, it cannot replace a forward slash (/).<br><br>Use ? within or at the end of a phrase.<br><br>Examples:<br><br>The query **cell?** searches names containing **cell**+**<one additional character>**. (cells and cello, but not cell)<br><br>The query **.xl?** searches names containing **.xl**+**<a third character>**. (.xls or .xlr)<br><br>The query **wom?n** searches names containing **wom**+**<a fourth character>**+**n**. (woman or women)<br><br>The query **carbon fib??** searches names containing **carbon fib**+**<two characters>**. (carbon fiber or carbon fibre) |
| *****<br><br>**Zero or more characters** | Substitutes zero or more characters or can be used to truncate multiple characters. Use * for alternative spellings and an unlimited number of characters within a word.<br><br>If used in a path, it cannot replace a forward slash (/).<br><br>Examples:<br><br>The query **behavi*r** searches names containing **behavi**+**<any character or number of characters>**+**r**. (behaviour, behavior, or behavi123.zr) |

© 2015

| Wildcard | Description |
|---|---|
| | The query **patent*** searches names containing **patent+<a character or any number of characters>**. ( patents, patentable, patented, patent123)<br><br>The query **patent*.jpg** searches names containing **patent+<a character or any number of characters>+.jpg**.<br><br>(patents.jpg, patentable.jpg, patented.jpg, patent123. jpg, etc; ***.jpg** substitutes for only all names containing **<any character or set of characters>+.jpg** |
| ***?**<br><br>**One or more characters** | Substitutes a minimum number or more characters. The minimum number of characters matched is equal to the number of ? that follow the *.<br><br>*?? substitutes for at least two characters.<br><br>*??? substitutes for at least three characters, and so on.<br><br>If used in a path, it cannot replace a forward slash (/).<br><br>Use *? within or at the end of a word.<br><br>Examples:<br><br>The query **carbon fib*??** searches for carbon fiber, carbon fibre, carbon fibers, carbon fibres, and carbonfib123.<br><br>The query **actua*????** searches for filenames containing **actua+<four or more additional characters>**. (actuarial, actuaries, actualization, actua12345.xls, but not actual) |
| **#**<br><br>**Zero or more characters in a pathname, including slashes** | Substitutes for zero or more characters in a path name; valid for use only within a path.<br><br>Use to denote the forward slash (/).<br><br>Example:<br><br>The query **document#Q42007** searches for **document+<any character, including slashes or no character>+Q42007**. (documentQ42007, documentsQ42007, document1Q42007, and document/Q42007) |

© 2015

| Wildcard | Description |
|---|---|
| **#?**<br><br>**One or more characters in a pathname, including slashes** | Substitutes for a minimum number or more characters in a path name; valid for use only within a path. The minimum number of characters matched is equal to the number of ? that follow the #.<br><br>Matches the forward slash (/).<br><br>Example:<br><br>The query **document#?Q42007** searches for **document+<any character, including slashes>+ Q42007**. (documentsQ42007, document/Q42007, and documents/123Q42007) |
| **[ ]**<br><br>**Set of characters** | Substitutes a set and includes any one of the characters in the set. Or, an ASCII sequential run of characters can be indicated by using a hyphen to separate the first character in the sequence from the last character in the sequence: [<beginning character>-<end character>].<br><br>Examples:<br><br>The query **[afe]** matches a, f, or e.<br><br>The query **[a-m]** matches any single character in the range of a to m. |
| **[!]**<br><br>**Characters not in set** | Substitutes any one character that is not specified in a set. Or, an ASCII sequential run of characters can be indicated by using a hyphen to separate the first character in the sequence from the last character in the sequence: [!<beginning character>-<end character>].<br><br>Examples:<br><br>The query **[!afe]** searches for any single character other than a, f, or e.<br><br>The query **[!a-m]** searches for any single character that is not in the range of a-m. |
| **!**<br><br>**Entire pattern not in set** | When **!** is the first character of a pattern, the entire pattern is omitted.<br><br>Example:<br><br>The query **!primary** returns everything except "primary". |

© 2015

| Wildcard | Description |
|---|---|
| | When using this wildcard in extended metadata searches, it is best to use "is equal to". To obtain predictable results, avoid "contains", "does not contain", and "is not equal to." |
| \<br>**Escape next character** | Causes the character following the backslash to be treated as a literal character. Normally, this is used with one of the wildcard characters to denote that character itself, not its wildcard expression meaning.<br>Example:<br>To process **Accounting*2007**, type **Accounting*2007** since * is normally interpreted by the Information Repository as a wildcard. |
| **Multiple wildcards** | Along with using wildcards individually, combine them to create powerful filters and search criteria.<br>Example:<br>The query **[abc]*.xls** searches any phrase beginning with **a**, **b**, or **c+<any character or number of characters>+.xls**.<br>The query **[!abc]*.xls** searches any phrase not beginning with **a**, **b**, or **c+<any character or number of characters>+.xls**.<br>The query **and*.???** searches **and+<any number of characters>+.+any three characters**. |

## More POSIX Standard Wildcard Examples

The examples in the following table illustrate contrast in the way wildcards function differently from one another.

| Wildcard | Sample Phrase | Matches | Does not match |
|---|---|---|---|
| **?**<br>**Any single character in a name** | path?.doc | path1.doc<br>paths.doc<br>pathq.doc<br>etc. | path<br>path/.doc<br>path.doc<br>path_sample.doc<br>etc. |

© 2015

| Wildcard | Sample Phrase | Matches | Does not match |
|---|---|---|---|
| *****<br>**Zero or more characters in a name** | path*.doc | path.doc<br>path1.doc<br>path_sample.doc<br>etc. | path<br>path/1.doc<br>path1.docs<br>etc. |
| ***?**<br>**One or more characters in a name** | path*?.doc | path1.doc<br>paths.doc<br>path_sample.doc<br>etc. | path<br>path.doc<br>path/.doc<br>etc. |
| **#**<br>**Zero or more characters in a pathname, including slashes** | path#.doc | path.doc<br>path1.doc<br>path_sample.doc<br>path/1.doc<br>etc. | path<br>path1.docs<br>sample/path.doc<br>etc. |
| **#?**<br>**One or more characters in a pathname, including slashes** | path#?.doc | path1.doc<br>path_sample.doc<br>path/1.doc<br>etc. | path<br>path.doc<br>path1.docs<br>etc. |
| **[ ]**<br>**Set of characters** | path[1-3].doc | path1.doc<br>path2.doc<br>path3.doc | path<br>path.doc<br>path.docs<br>path4.doc<br>path5.doc<br>patha.doc<br>pathq.doc<br>etc. |
| **[!]**<br>**Characters not in set** | path[!1,2,3].doc | path0.doc<br>path4.doc | path1.doc<br>path2.doc |

© 2015

| Wildcard | Sample Phrase | Matches | Does not match |
|---|---|---|---|
| | | path5.doc<br>patha.doc<br>pathq.doc<br>etc. | path3.doc<br>path<br>path.doc<br>path.docs<br>etc. |
| **!**<br>**Entire pattern not in set** | !path.doc | all other files in repository | !path.doc |

## Regular Expressions (Content Searching)

Use regular expressions to search for specific content or text manipulation.

The following are things to keep in mind when using the standard wildcards:

- With or without quotation marks, search is not case sensitive.
- These wildcard operators do not work for file or directory search and filtering (you must use the POSIX standard wildcards).

### Regular Expressions Table for Content Searching

This functionality allows you to put limitations on files that are processed to those containing a particular word or phrase.

**Quotation marks** - To process only files that contain a specific phrase, be sure to enclose the phrase in quotation marks. Otherwise, all files containing any word typed is processed in the query. For example, if searching "Information Repository", only files that contain the complete phrase "Information Repository" are processed. In contrast, without quotation marks in place, any file containing Information Repository, Repository Information, Information, or Repository are processed.

The table below lists all the wildcard operators only for content searching.

| Wildcard | Description |
|---|---|
| **?**<br>**Any single character** | Substitutes a single character or can be combined to represent multiple characters. Use the ? for specific alternative spellings.<br>? substitutes a single character<br>?? substitutes two characters |

© 2015

| Wildcard | Description |
|---|---|
| | ??? substitutes three characters, and so on.<br><br>If used in a path, it cannot replace a forward slash (/).<br><br>Use ? within or at the end of a phrase.<br><br>Examples:<br><br>The query **cell?** searches names containing **cell**+**<one additional character>**. (cells and cello, but not cell)<br><br>The query **.xl?** searches names containing **.xl**+**<a third character>**. (.xls or .xlr)<br><br>The query **wom?n** searches names containing **wom**+**<a fourth character>**+**n**. (woman or women)<br><br>The query **carbon fib??** searches names containing **carbon fib**+**<two characters>**. (carbon fiber or carbon fibre) |
| *****<br><br>**Zero or more characters** | Substitutes zero or more characters or can be used to truncate multiple characters. Use * for alternative spellings and an unlimited number of characters within a word.<br><br>If used in a path, it cannot replace a forward slash (/).<br><br>Examples:<br><br>The query **behavi*r** searches names containing **behavi**+**<any character or number of characters>**+**r**. (behaviour, behavior, or behavi123.zr)<br><br>The query **patent*** searches names containing **patent**+**<a character or any number of characters>**. ( patents, patentable, patented, patent123)<br><br>The query **patent*.jpg** searches names containing **patent**+**<a character or any number of characters>**+**.jpg**.<br><br>(patents.jpg, patentable.jpg, patented.jpg, patent123.jpg, etc; ***.jpg** substitutes for only all names containing **<any character or set of characters>**+**.jpg** |
| ***?**<br><br>**One or more characters** | Substitutes a minimum number or more characters. The minimum number of characters matched is equal to the number of ? that follow the *.<br><br>*?? substitutes for at least two characters. |

© 2015

| Wildcard | Description |
|---|---|
| | *??? substitutes for at least three characters, and so on.<br><br>If used in a path, it cannot replace a forward slash (/).<br><br>Use *? within or at the end of a word.<br><br>Examples:<br><br>The query **carbon fib*??** searches for carbon fiber, carbon fibre, carbon fibers, carbon fibres, and carbonfib123.<br><br>The query **actua*????** searches for filenames containing **actua+<four or more additional characters>**. (actuarial, actuaries, actualization, actua12345.xls, but not actual) |
| **~**<br><br>**Proximity searches** | Use a proximity search to find words that are within proximity to one another. To execute, use **~** (the tilde symbol) and a value at the end of a phrase.<br><br>Example:<br><br>To query for "**compliance**" and "**December**" within 10 words of each other use **compliance December~10**. |
| **~**<br><br>**Fuzzy searches** | Use a fuzzy search to find an approximate spelling. To execute, use **~** (the tilde symbol) at the end of a single term.<br><br>Example:<br><br>To query for a term similar in spelling to "**report**" use **report~**. This search find terms like deport, reports, and reporting.<br><br>You can specify the level of similarity. Using a value between 0 and 1, only terms with a higher similarity are matched with values closer to 1. For example, **roam~0.8**. The default is 0.5 if a value is not defined. |
| **[]**<br><br>**{}**<br><br>**Range searches (TO)** | Use range searches to match documents where field values are between the lower and upper limits specified by the search, and the searches can be inclusive or exclusive of the limits. Inclusive range searches are marked by brackets. Exclusive range searches are marked by curly braces.<br><br>Example: |

© 2015

| Wildcard | Description |
|---|---|
| | To query a date, **mod_date:[20020101 TO 20030101]** finds files whose mod_date fields have values between 20020101 and 20030101, inclusive.<br><br>To query a non-date, **title:{accounting TO sarbanes}** finds files whose titles are between **accounting** and **sarbanes**, but excluding **accounting** and **sarbanes**. |
| **^**<br><br>**Boosting a term** | Control the relevance of a document by boosting the value of a specific term to search for.<br><br>To boost a term, use **^** (the caret symbol) with a boost factor (a number) at the end of the search term. The higher the boost factor, the more relevant the returned term will be. By default, the boost factor is 1. Although the boost factor must be positive, it can be less than 1 (for example, 0.2).<br><br>Example:<br><br>To query **corporate compliance** and you want the term **compliance** to appear more relevant, boost it using **^** along with the boost factor next to the term. Type **corporate compliance^4**.<br><br>Boost phrase terms by enclosing a phrase in quotation marks. **"corporate compliance"^4** |
| **OR**<br><br>**AND, &&**<br><br>**+**<br><br>**NOT, !, -**<br><br>**boolean operators** | Boolean operators allow terms to be combined through logic operators. **AND**, **OR**, **+**, and **NOT** are supported as boolean operators.<br><br> Boolean operators must be in capital lettering.<br><br>**OR**<br><br>OR links two terms and finds a matching document when either of the terms exist in a document. **||** can be used in place of OR. OR is the default conjunction operator, meaning that if there is no boolean operator between two terms, OR is assumed.<br><br>Example:<br><br>To query documents that contain **corporate compliance** or **compliance**, you would use **"corporate compliance" OR compliance**. The quotes indicate a single phrase.<br><br>**AND** |

© 2015

| Wildcard | Description |
| --- | --- |
| | AND matches documents where both terms exist anywhere in the text of a single document. && can be used in place of AND.<br><br>Example:<br><br>To query documents that contain **corporate compliance** and **Second Quarter 2007,** use **"corporate compliance" AND "Second Quarter 2007"**. The quotes indicate a single phrase.<br><br>**+**<br><br>The plus symbol requires that the term after + exists somewhere in a single file.<br><br>Example:<br><br>To query files that contain **compliance** and may contain **corporate** you would use **corporate + compliance**.<br><br>**NOT**<br><br>NOT excludes documents that contain the term after NOT. **!** (exclamation point) or **-** (minus symbol) can be used in place of NOT.<br><br>NOT cannot be used with just one term.<br><br>Example:<br><br>To query documents that contain **corporate** but not **compliance** use, **corporate NOT compliance**.<br><br>**Grouping**<br><br>To control the boolean logic for a query, use parentheses to group clauses to form sub queries.<br><br>Example:<br><br>To query for either **corporate** or **compliance** and **Second Quarter 2007** you would use **(corporate OR compliance) AND "Second Quarter 2007"**. This ensures the phrase after AND must exist and either term within the parentheses may exist.<br><br>**Field Grouping**<br><br>Use parentheses to group multiple clauses to a single field. |

© 2015

| Wildcard | Description |
|---|---|
| | Example:<br><br>To query a file containing both **return** and the phrase **overdue accounts** you would use **title: (+return +"overdue accounts")**. |
| \<br><br>**Escaping special characters** | Escaping special characters can be a part of the query syntax. Special characters are:<br><br>**+ - && \|\| ! ( ) { } [ ] ^ " ~ * ? : **<br><br>To execute a search using these characters literally (to escape any of these character), use \ before the character.<br><br>Example:<br><br>To query for **(1+1):2**, use **\(1\+1\)\:2**. In this case, if you do no use the escape character for **(1+1):2**, the query would search for **( OR 1 OR AND 1 OR ) OR : OR 2**.<br><br> It is recommended to avoid using characters that Phoenix RSM interprets as special. If you need to use a character literally that Phoenix RSM uses as a wildcard, the character must be preceded by an escape character ( \ ). |

# Filters

The two main types of filters used in Phoenix RSM are file and directory and can be applied in several of the product applications. Use filters to pinpoint the inclusion or exclusion of specific (or groups) of files or directories. Wildcards may also be used when formulating a filter. For more information, see Wildcards.

File filters operate on file names and directory filters operate on directory names. If a policy features both file and directory files, then both types are used. File filters and directory filters can complement each other but the product processes them separately, first applying any directory filters and then applying any file filters.

**Exclude filters** - Implies "include all", meaning that everything is processed in the job unless files or directories are explicitly excluded.

**Include filters** - Implies "exclude all", meaning that only the files or directories specified by an include filter are included in a job.

© 2015

Filters process exactly what you type. For example, if you create an include filter for **.doc**, then the processed files are literally named **.doc**. If you want to process all files that are of a .doc type, the filter would include a wildcard: ***.doc**.

### File Filters

If a file filter does not have a path delimiter, the product matches the pattern against the last leaf of the path, which is the file name itself. If the file filter does have a path delimiter, the product matches the pattern against the entire path, including the file name.

File filters are read from the top down. For example, if you have an exclude file filter that excludes all .jpg files followed by a filter that includes all .jpg files, the .jpg files are excluded.

### Directory Filters

If a directory filter does not have a path delimiter, the product tries to match the pattern against the last leaf of the path separately and looks for the first match. If a directory filter does have a path delimiter, the product matches the pattern against the entire path.

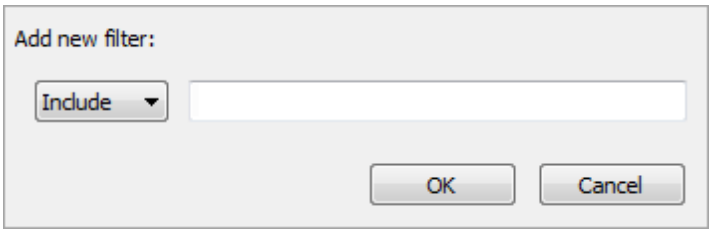
Directory filters are read from the top down. For example, if you have an exclude directory filter that excludes all folders named Pictures followed by a filter that includes Pictures/2003Convention, the first filter takes precedence and Pictures/2003Convention is not included.

When typing paths or path searching patterns, use the forward slash (/).

## Create File Filters and Directory Filters

File filters enable you to include or exclude particular files by file name or file type. Directory filters enable you to include or exclude directories and their contents. It is possible to use file and directory filters at the same time.

1. In the **Files to Include/Exclude** or **Directories to Include/Exclude** group, click the **Add** button.



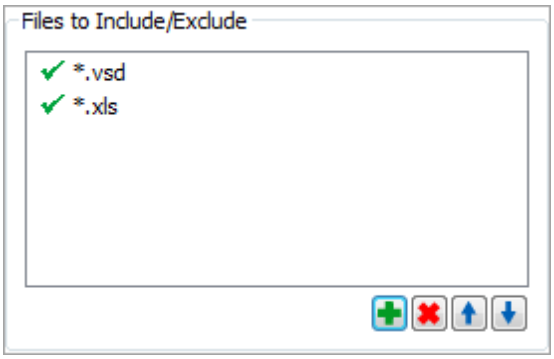

2. Select a filter type. Use **Include** to ensure the inclusion of files, directories, and file types. Use **Exclude** to exclude files, directories, and file types. This text box supports characters, numbers, and symbols needed to define filters.

© 2015

3. Type a filter, and then click **OK**. For example, in the **Files to Include/Exclude**, if you type *.vsd and then *.xls, the text box would appear as follows. Include filters are preceded by a ✔ green check mark, and exclude filters by a ✘ red x.

   The **Files to Include/Exclude** or **Directories to Include/Exclude** group boxes display the values entered from the Add Filter dialog box. Wildcards are supported.

   To assign priority to filters, move them up and down using the up arrow button and down arrow button.




## Delete File Filters and Directory Filters

In the **Files to Include/Exclude** or **Directories to Include/Exclude** group, select a filter, and click the **Delete** button.

## Understanding Directory Filters

The following table demonstrates how directory filters work and includes some uses of wildcards.

Filter - The filter applied in the Criteria tab. This can be either an Include or Exclude filter.

Pathname - The current file or directory being looked at to determine the next step of processing.

Process? - Determine if the file or directory at that pathname is a match to the applied filter. If Yes, use the Include/Exclude value of the filter to determine the final process value. If No, the directory can still be walked to look for further matches.

Walk? - Determine if the tree will be walked further down in search of a match. Files are never walked.

© 2015

| Filter | Pathname | Process? | Walk? |
|---|---|---|---|
| **//H1/#** | //H1 | No | Yes |
| | //H1/D1 | Yes | Yes |
| | //H1/D1/F1 | Yes | No |
| **//H1#** | //H1 | No | Yes |
| | //H1/D1 | Yes | Yes |
| | //H1/D1/F1 | Yes | No |
| **//H1/D1/D2/#** | //H1/D1 | No | Yes |
| | //H1/D1/D2 | No | Yes |
| | //H1/D1/D2/D3 | Yes | Yes |
| | //H1/D1/D2/F1 | Yes | No |
| | //H1/D1/D2/D3/F1 | Yes | No |
| | //H2/D1 | No | No |
| **//H1/D1** | //H1/D1 | Yes | Yes |
| | //H1/D1/F1 | Yes | No |
| | //H1/D1/D2 | Yes | No |
| | //H1/D1/D2/F1 | No | No |
| **//H1/*** | //H1/D1 | Yes | Yes |
| | //H1/F1 | Yes | No |
| | //H1/D1/D2/D3 | No | No |
| **//H1/D1/D2/*** | //H1/D1/D2/D3 | Yes | Yes |
| | //H1/D1/D2/D3/D4 | No | No |
| | //H1/D1/D2/D3/F1 | No | No |
| | //H1/D1/D2/F1 | Yes | No |
| | //H1 | No | Yes |
| | //H1/D1 | Yes | Yes |

© 2015

H = Host

D = Directory

F = File

## Understanding File Filters

The following table demonstrates how file filters work and includes some uses of wildcards. If Process? is Yes, use the Include/Exclude value of the filter to determine the final process value.

Filter - The filter applied in the Criteria tab. This can be either an Include or Exclude filter.

Pathname - The current file or directory being looked at to determine the next step of processing.

Process? - Determine if the file or directory at that pathname is a match to the applied filter. If Yes, use the Include/Exclude value of the filter to determine the final process value. If No, the directory can still be walked to look for further matches.

Walk? - Determine if the tree will be walked further down in search of a match. Files are never walked.

| Filter | Pathname | Process? | Walk? |
|---|---|---|---|
| **//H1/#** | //H1/D1/F1 | Yes | No |
| **//H1#** | //H1/D1/F1 | Yes | No |
| **//H1/D1/D2/#** | //H1/D1/D2/F1 | Yes | No |
| | //H1/D1/D2/D3/F1 | Yes | No |
| **//H1/D1/D2/*** | //H1/D1/D2/D3/F1 | No | No |
| | //H1/D1/D2/F1 | Yes | No |
| **D1** | //H1/D1/F1 | Yes | No |
| **D2** | //H1/D1/D2/D3/F1 | Yes | No |
| | //H1/D1/F1 | No | No |

H = Host

D = Directory

F = File

## Filter Examples

© 2015

If you had a directory that contained several different file types and you want to process all of the files in the directory except .jpg files, you can create an exclude filter for files with a .jpg extension. In the following example, ✘ denotes "exclude"; * (asterisk) is the wildcard symbol for "all"; .jpg is the file extension subject to the prefixed symbols. The left column lists all the directory files, the center column shows the applied filter, and the right column shows the processed files. Notice that the .jpg files are not processed.

| Files in specified directory | Filter | Files that are processed |
|---|---|---|
| Elevator design 12502.vsd | ✘*.jpg | Elevator design 12502.vsd |
| Elevator design rev 20502.vsd | | Elevator design rev 20502.vsd |
| Elevator design rev 21502.vsd | | Elevator design rev 21502.vsd |
| Part345X.xls | | Part345X.xls |
| Part236.xls | | Part236.xls |
| Part 532.xls | | Part 532.xls |
| Ref-guide rev21502.doc | | Ref-guide rev21502.doc |
| Ref-guide rev21802.doc | | Ref-guide rev21802.doc |
| Install guide 21502.ind | | Install guide 21502.ind |
| Illustration 532.psd | | Illustration 532.psd |
| Illustration 236.psd | | Illustration 236.psd |
| Vacation 1.jpg | | |
| Vacation 2.jpg | | |
| Vacation 3.jpg | | |

Filter strings can contain wildcard symbols, making the Information Repository very flexible. Use several filters together to create almost any include/exclude combination.

Using the same file set as an example, the only files processed are the .vsd and .xls files.

© 2015

| Files in specified directory | Filter | Files that are processed |
|---|---|---|
| Elevator design 12502.vsd | ✔ *.vsd | Elevator design 12502.vsd |
| Elevator design rev 20502.vsd | ✔ *.xls | Elevator design rev 20502.vsd |
| Elevator design rev 21502.vsd | | Elevator design rev 21502.vsd |
| Part345X.xls | | Part345X.xls |
| Part236.xls | | Part236.xls |
| Part 532.xls | | Part 532.xls |
| Ref-guide rev21502.doc | | |
| Ref-guide rev21802.doc | | |
| Install guide 21502.ind | | |
| Illustration 532.psd | | |
| Illustration 236.psd | | |
| Vacation 1.jpg | | |
| Vacation 2.jpg | | |
| Vacation 3.jpg | | |

# ExportExtensions.cfg

Use an ExportExtensions.cfg text file to customize your export options for files that have been retrieved. This is done by configuring fields seen in export retrieval options for the Phoenix RSM search applications. This capability is intended only for advanced users.

- Create an ExportExtensions.cfg using any text editor and save as a plain text document. Once created, it needs to be added to the following path: <install-dir>\Config. See Create an ExportExtensions.cfg - example.
- ExportExtensions.cfg is a block structured text file. At the end of this section, there is a sample ExportExtensions.cfg. You can implement the file as is (at the path noted above), or modify the file to meet your own criteria and then implement it.

ExportExtensions.cfg is comprised of at least one or more ExportExtension blocks. An ExportExtension block has two main sections:

- Command
- Query

## Command Section of the Export Extensions Block

© 2015

The Command section of the block extends from the words "ExportExtension" to the command specification (in the example below). It includes the ExportExtension statement that defines the beginning of an ExportExtension block and includes the execute command and other tokens:

```
ExportExtension #  This identifies the beginning of the ExportExtension block.
[ # This is the opening brace for the ExportExtension block.

    <token>=<value>
    <token>=<value>

    Command = <%# %# %# %# ... %U %M ...> # This is REQUIRED statement.
```

The following block name defines the beginning of an ExportExtension block in an ExportExtensions.cfg file:

| Block name | Description |
|---|---|
| ExportExtension | The beginning of an ExportExtension block.<br><br>Required. |

Note that the entire block is ignored if there are fewer Query block statements than %# in the Command. For example, if you have three Query block sections and four %#, then the block will not be read.

| Command | Description |
|---|---|
| Command = <*command specification*> | Define the execute command specification. Along with the command, the command line must enumerate each Query block. See the sample file below for an illustration.<br><br>Required.<br><br>**%#** is the substitution query value (where # is a number). Each %# enumerates a Query, one %# per Query, and can be in any order. The command specification cannot have more %# than Query statements, but you can specify certain blocks by omitting query numbers. For example, to include only query blocks 1, 3, and 7, use <%1, %3, %7><br><br>The following substitution tokens may also be in the Command specification:<br><br>• %U = User<br>• %M = Host |

© 2015

| Command | Description |
|---|---|
| | • %D = Date<br>• %T = Time<br>• %P = Path to where the files are retrieved<br>• %O = Filename containing list of files in the export list. |

Use tokens to define optional functionality in the Command section. Unless noted, tokens are not necessary. When tokens are omitted, default values are used. Include any of the following tokens when you want to use non-default values:

| Token/Value | Description |
|---|---|
| DeleteWhenDone = <*boolean*> | Define if files are to be deleted from the local system when the command is complete.<br>Valid values = true \| false<br>Default = true |
| Description = <*character string*> | The tool tip for the label.<br>Default = "" |
| DestinationPathname = <*pathname*> | The path to where the files are exported.<br>Default = "" |
| FileNaming = <*alpha*> | Define how files are named.<br>Valid values = Original \| AtSelection \| FilenameOnly.<br>Default = Original |
| Label = "<*character string*>" | The label found in the **Export Destination** box.<br>Default = Export Extension |
| Overwrite = <*alpha*> | When files are overwritten.<br>Valid values = Never \| Always \| IfNewer<br>Default = Never |
| RestoreSecurity = <*boolean*> | Define if original security settings are restored.<br>Valid values = true \| false |

© 2015

| | |
|---|---|
| | Default = true |
| RestoreTimes = <*boolean*> | Define times it is used.<br>Valid values = true \| false<br>Default = true |

## Query section of the Export Extensions Block

Query block statements describe the controls that appear on the application. You may have any number of queries.

```
    Query
    [
           <token>=<value>
           <token>=<value>
           <token>=<value>
           <token>=<value>
           <token>=<value>
           <token>=<value>
    ]

    Query
    [
           <token>=<value>
           <token>=<value>
           <token>=<value>
           <token>=<value>
           <token>=<value>
           <token>=<value>
    ]
] # This is the closing brace for the ExportExtension block.
```

The following block name defines the beginning of a Query block in an ExportExtensions.cfg file.

| Block name | Description |
|---|---|
| Query | The beginning of a Query block.<br>Required |

The following tokens can be used in Query blocks:

| Query block Type | Valid Token/Values | Description |
|---|---|---|
| **Checkbox** | Name = "<*character string*>" | The export item's name.<br>Required<br>Default = "" |
| | Type = Checkbox | The Query type. |
| | Label = "<*character string*>" | The label for the control as it will appear in the application.<br>Default = "" |
| | DefaultValue = <*boolean*> | The value to load into the control by default.<br>Valid values = true \| false<br>Defaults = true (checked) |
| | Description = "<*character string*>" | The tooltip for the control.<br>Default = "" |
| **Choice** | Name = "<*character string*>" | The export item's name.<br>Required<br>Default = "" |
| | Type = Choice | The Query type. |
| | Label = "<*character string*>" | The label for the control as it will appear in the application.<br>Default = "" |
| | DefaultValue = <*number*> | The value to load into the control by default.<br>Valid values = the number of the entry in the drop-down list<br>Default = the first choice listed.<br> If the DefaultValue for a Choice block is greater than the number of Choices entered, the entire ExportExtension block is ignored. |

© 2015

| Query block Type | Valid Token/Values | Description |
|---|---|---|
| | BlankValueOk = <*boolean*> | Indicate if the value is left blank. Valid for String, Pathname, and Choice only.<br>Valid values = true \| false<br>Default = true |
| | Description = "<*character string*>" | The tooltip for the control.<br>Default = "" |
| | Choice = "<*character string*>" | A choice statement that can be selected. Must have at least one choice. Can be reused as many times as needed. |
| **Pathname** | Name = "<*character string*>" | The export item's name.<br>Required<br>Default = "" |
| | Type=Pathname | The Query type. |
| | Label = "<*character string*>" | The label for the control as it will appear in the application.<br>Default = "" |
| | DefaultValue = "<*character string*>" | The value to load into the control by default.<br>Valid value= a string<br>Default = "" |
| | BlankValueOk = <*boolean*> | Indicate if the value is left blank. Valid for String, Pathname, and Choice only.<br>Valid values = true \| false<br>Default = true |
| | Description = "<*character string*>" | The tooltip for the control.<br>Default = "" |
| **Spin** | Name = "<*character string*>" | The export item's name. |

© 2015

| Query block Type | Valid Token/Values | Description |
|---|---|---|
| | | Required<br>Default = "" |
| | Type = Spin | The Query type. |
| | Label = "<*character string*>" | The label for the control as it will appear in the application.<br>Default = "" |
| | DefaultValue = <*number*> | The value to load into the control by default.<br>Valid values = a number between the LowerLimit and UpperLimit<br>Default = the lower limit<br> If the DefaultValue for a Spin block is not between the LowerLimit and UpperLimit, the entire ExportExtension block is ignored. |
| | Description = "<*character string*>" | The tooltip for the control.<br>Default = "" |
| | LowerLimit = <*number*> | The lower limit for the spin control.<br>Default = 0 |
| | UpperLimit = <*number*> | The upper limit for the spin control. Valid only for Spin.<br>Default = lower limit + 100 |
| **String** | Name = "<*character string*>" | The export item's name.<br>Required<br>Default = "" |
| | Type = String | The Query type. |
| | Label = "<*character string*>" | The label for the control as it will appear in the application. |

© 2015

| Query block Type | Valid Token/Values | Description |
|---|---|---|
| | | Default = "" |
| | DefaultValue = "<*character string*>" | The value to load into the control default.<br>Valid values = a string<br>Defaults = "" |
| | BlankValueOk = <*boolean*> | Indicate if the value is left blank. Valid for String, Pathname, and Choice only.<br>Valid values = true \| false.<br>Default = true |
| | Description = "<*character string*>" | The tooltip for the control.<br>Default = "" |

### A Note About Wildcards

Pay attention to brackets [ ]; there needs to be an opening bracket [ after "ExportExtensions" and a closing bracket ] after the last Query block.

It is best to get familiar with Phoenix RSM's wildcard characters. If you need to use a character that is used by Phoenix RSM as a wildcard, the character must be preceded by an escape character ( \ ). For example, *This is an example using escape characters in a statement with a wildcard*.

The following are Phoenix RSM wildcards and special characters: **?**, *****, **#**, **!**, **~**, **^**, **&**, **[ ]**, **{ }**, \, **"**.

For more information see Wildcards.

## Create an ExportExtensions.cfg - Example

1. Open a text editor, such as WordPad or Notepad, and start a new document. If using WordPad, be sure to create a Text Document (.txt) and not Rich Text Format (.rtf).

2. Copy and paste the following ExportExtensions.cfg sample file into the new document.

```
# This name is significant and identifies this as an ExportExtension block.
ExportExtension
[
    Description = "Custom"
```

© 2015

```
Label = "Custom"

# This is a REQUIRED statement in an Export Extension block.
Command = "echo %1 %2 %3 %4 %5 %6 %P %U %M %D %T"

Query
[
       Name         = "CaseName"
       Type         = String
       Label        = "Case Name"
       DefaultValue = ""
       BlankValueOk = true
       Description  = "What is the name of the case?"
]

Query
[
       Name         = "AgentName"
       Type         = Choice
       Label        = "Agent Name"
       BlankValueOk = true
       Description  = "What is the Agent's name?"
       Choice       = "John Napoli"
       Choice       = "Katie Aguilar"
       Choice       = "Justin Campbell"
]

Query
[
       Name         = "AgentId"
       Type         = Spin
       Label        = "Agent ID"
       DefaultValue = 1001
       Description  = "The ID number of the agent."
       LowerLimit   = 1000
       UpperLimit   = 5000
]

Query
[
       Name         = "CaseType"
       Type         = Choice
       Label        = "Case Type"
       Description  = "What is the case type?"
       Choice       = "Arson"
       Choice       = "Theft"
       Choice       = "Narcotics"
]

Query
[
```

```
            Name         = "APathname"
            Type         = Pathname
            Label        = "Pathname"
            DefaultValue = ""
            BlankValueOk = false
            Description  = ""
      ]

      Query
      [
            Name         = "InclueMd"
            Type         = Checkbox
            Label        = "Include content metadata?"
            DefaultValue = false
            Description  = "Include all customer metadata?"
      ]
]
```

3. Save the document to <install-dir>/Config, naming it **ExportExtensions.cfg**.
4. Launch your Phoenix RSM search application.
5. Set the Export Destination. The values for your custom export options are the same as those in your ExportExtensions.cfg file.

   In ExportExtensions.cfg, backslash ( \ ) is used as an escape character. Use \ whenever you type characters, such as quotation marks, that Phoenix RSM interprets as code. For example, ExportExtensions.cfg contains the following line: Sample Value for the \"How do you want to export the retrieved files?\" field. In this line, each backslash tells Phoenix RSM that the next character is literal, not a command. While ExportExtensions.cfg contains Sample Value for the \"How do you want to export the retrieved files?\", the Export Job Configuration pane displays Sample Value for the "How do you want to export the retrieved files?" (notice, no backslashes).
6. Close the application.

Once this file is created, you can go back and modify it at any time with different or additional variables. See the above sections for tokens/values to change or add.

# MetadataExtensions.cfg

## Create a MetadataExtensions.cfg

- Create a MetadataExtensions.cfg using any text editor, such as Notepad, Text Edit, WordPad. Be sure to create a Text Document (.txt) and not Rich Text Format (.rtf).
- MetadataExtensions.cfg is a block structured text file.
- Once created, add it to the path: <install-dir>\Config.

© 2015

At the end of this section, find a sample MetadataExtensions.cfg. You can implement the file as is (at the path noted above) to see how it works or modify the file to meet your own criteria and then implement it.re.

### Metadata Extension Block Structure

The metadata extension block structure includes three blocks (IngestMdExt, ModMdExt, and SearchMdExt). Each comprised of one or more Query blocks.

Query block statements describe the controls to appear on the application. These can include any number of string fields, checkboxes, spin controls, path name boxes, and choice controls. Each block can have any number of Query blocks. It's best to ensure that the IngestMdExt block and SearchMdExt contain the same Query blocks since only ingested metadata is searched. However, the Query blocks contained in SearchMdExt can be limited to a subset of those in IngestMdExt. In this case, you would be able to search on the Query blocks listed in SearchMdExt.

Pay attention to brackets [ ]; for IngestMdExt, ModMdExt, and SearchMdExt, there needs to be an opening bracket after "<Extension>" and a closing bracket after its last Query block.

If a Query block contains an error, the entire metadata extension block (IngestMdExt, SearchMdExt, ...) is ignored.

In the following example, note that tokens cannot be used in Query blocks indiscriminately. Each Query block supports only specific tokens. See **Valid Token/Values for Query Blocks** below for details.

```
#  This identifies the beginning of the block.
<block identifier>

# This is the opening brace for the block.
[

    Query
    [
           <token>=<value>
           <token>=<value>
           <token>=<value>
           <token>=<value>
           <token>=<value>
           <token>=<value>
    ]

    Query
    [
           <token>=<value>
           <token>=<value>
           <token>=<value>
           <token>=<value>
           <token>=<value>
           <token>=<value>
    ]
```

```
]
# This is the closing brace for the block.
```

## Blocks

The following are the blocks used in MetadataExtensions.cfg:

| Block Identifier | Description |
|---|---|
| IngestMdExt | The beginning of the metadata extensions block for Phoenix RSM ingesting and capturing applications. May not contain a SearchMdExt block or ModMdExt block.<br><br>Required. |
| ModMdExt | The beginning of the "edit metadata" metadata extension block for Phoenix RSM search and retrieve applications. May not contain an IngestMdExt block or SearchMdExt block.<br><br>Required. |
| SearchMdExt | The beginning of the metadata extensions block for Phoenix RSM search and retrieve applications. It may not contain an IngestMdExt block or ModMdExt block.<br><br>Required. |
| Query | The beginning of a Query block contained within a metadata extensions block.<br><br>Required.<br><br> As illustrated in the examples below, Query blocks must be contained within metadata extension blocks (SearchMdExt and IngestMdExt). |

### Valid Token/Values for Query Blocks

The tokens in the table below can be used only in Query blocks. Although the IngestMdExt, ModMdExt, and SearchMdExt blocks use the same types of Query blocks, each must have its own individual Query blocks.

© 2015

It is best to avoid using characters that Phoenix RSM interprets as wildcards or as otherwise special. If you need to use one of these characters, then the character must be preceded by an escape character ( \ ).

For example, *This is an example using escape characters in a statement with a wildcard*.

The following are wildcards and special characters: ?, *, #, !, ~, ^, &, [ ], { }, \, ". For more information see Wildcards.

| Query block Type | Valid Token/Values | Description |
|---|---|---|
| **Checkbox** | Name = "<*character string*>" | The metadata item's name.<br>Required<br>Default = "" |
| | Type = Checkbox | The Query type. |
| | Label = "<*character string*>" | The label for the control as it will appear in the application.<br>Default = "" |
| | DefaultValue = <*boolean*> | The value to load into the control by default.<br>Valid values = true \| false<br>Defaults = true (checked) |
| | Description = "<*character string*>" | The tooltip for the control.<br>Default = "" |
| **Choice** | Name = "<*character string*>" | The metadata item's name.<br>Required<br>Default = "" |
| | Type = Choice | The Query type. |
| | Label = "<*character string*>" | The label for the control as it will appear in the application.<br>Default = "" |
| | DefaultValue = <*number*> | The value to load into the control by default.<br>Valid values = the number of the entry in the drop-down list |

© 2015

| Query block Type | Valid Token/Values | Description |
|---|---|---|
| | | Default = the first choice listed.<br> If the DefaultValue for a Choice block is greater than the number of Choices entered, the entire MetadataExtensions block is ignored. |
| | BlankValueOk = <*boolean*> | Indicate if the value is left blank. Valid for String, Pathname, Date, and Choice only. A red asterisk will be displayed if this value is set to false.<br>Valid values = true \| false<br>Default = true |
| | Description = "<*character string*>" | The tooltip for the control.<br>Default = "" |
| | Choice = "<*character string*>" | A choice statement that can be selected. Must have at least one choice. Can be reused as many times as needed to create multiple choices to choose from. |
| | EditableChoice = <*boolean*> | Allow the user to edit a choice option.<br>Valid values = true \| false<br>Default = false |
| **Date** | Name = "<*character string*>" | The metadata item's name.<br>Required<br>Default = "" |
| | Type = Date | The Query type. |
| | Label = "<*character string*>" | The label for the control as it will appear in the application.<br>Default = "" |
| | DefaultValue = "<*character string*>" | The value to load into the control by default. |

© 2015

| Query block Type | Valid Token/Values | Description |
|---|---|---|
| | | Valid value = "" \| "today" to insert today's date \| "yyyy/mm/dd" for a chosen date<br>Default = "" |
| | BlankValueOk = <*boolean*> | Indicate if the value is left blank. Valid for String, Pathname, Date, and Choice only. A red asterisk will be displayed if this value is set to false.<br>Valid values = true \| false<br>Default = true |
| | Description = "<*character string*>" | The tooltip for the control.<br>Default = "" |
| **Pathname** | Name = "<*character string*>" | The metadata item's name.<br>Required<br>Default = "" |
| | Type = Pathname | The Query type. |
| | Label = "<*character string*>" | The label for the control as it will appear in the application.<br>Default = "" |
| | DefaultValue = "<*character string*>" | The value to load into the control by default.<br>Valid value = a string<br>Default = "" |
| | BlankValueOk = <*boolean*> | Indicate if the value is left blank. Valid for String, Pathname, Date, and Choice only. A red asterisk will be displayed if this value is set to false.<br>Valid values = true \| false<br>Default = true |
| | Description = "<*character string*>" | The tooltip for the control.<br>Default = "" |

© 2015

| Query block Type | Valid Token/Values | Description |
|---|---|---|
| **Spin** | Name = "<*character string*>" | The metadata item's name.<br>Required<br>Default = "" |
| | Type = Spin | The Query type. |
| | Label = "<*character string*>" | The label for the control as it will appear in the application.<br>Default = "" |
| | DefaultValue = <*number*> | The value to load into the control by default.<br>Valid values = a number between the LowerLimit and UpperLimit<br>Default = the lower limit<br> If the DefaultValue for a Spin block is not between the LowerLimit and UpperLimit, the entire MetadataExtensions block is ignored. |
| | Description = "<*character string*>" | The tooltip for the control.<br>Default = "" |
| | LowerLimit = <*number*> | The lower limit for the spin control.<br>Default = 0 |
| | UpperLimit = <*number*> | The upper limit for the spin control. Valid only for Spin.<br>Default = lower limit + 100 |
| **String** | Name = "<*character string*>" | The metadata item's name.<br>Required<br>Default = "" |
| | Type = String | The Query type. |

© 2015

| Query block Type | Valid Token/Values | Description |
|---|---|---|
| | Label = "<*character string*>" | The label for the control as it will appear in the application.<br>Default = "" |
| | DefaultValue = "<*character string*>" | The value to load into the control default.<br>Valid values = a string<br>Defaults = "" |
| | BlankValueOk = <*boolean*> | Indicate if the value is left blank. Valid for String, Pathname, Date, and Choice only. A red asterisk will be displayed if this value is set to false.<br>Valid values = true \| false<br>Default = true |
| | Description = "<*character string*>" | The tooltip for the control.<br>Default = "" |
| | NumLines = <*number*> | This value is the number of lines displayed for the textbox when using the string query. Use for multi-line metadata values.<br>Default = 1<br> This token is only for use with the IngestMdExt and ModMdExt sections. |

### Sample of Generic MetadataExtensions.cfg

```
# This name is significant and identifies this as an Metadata Extension block.
IngestMdExt
[
 Query
 [
      Name          = "CaseName"
      Type          = String
      Label         = "Case Name"
```

© 2015

```
     DefaultValue = ""
     BlankValueOk = true
     Description  = "What is the name of the case?"
          NumLines     = 2
]

Query
[
     Name         = "AgentName"
     Type         = Choice
     Label        = "Agent Name"
          BlankValueOk = true
     Description  = "What is the Agent's name?"
     Choice       = "John Napoli"
     Choice       = "Katie Aguilar"
     Choice       = "Justin Campbell"
          EditableChoice = true
]

Query
[
     Name         = "AgentId"
     Type         = Spin
     Label        = "Agent ID"
     DefaultValue = 1001
     Description  = "The ID number of the agent."
     LowerLimit   = 1000
     UpperLimit   = 5000
]

Query
[
     Name         = "CaseType"
     Type         = Choice
     Label        = "Case Type"
     Description  = "What is the case type?"
     Choice       = "Arson"
     Choice       = "Theft"
     Choice       = "Narcotics"
]

Query
[
          Name         = "A Pathname"
          Type         = Pathname
          Label        = "Pathname"
```

© 2015

```
          DefaultValue = ""
          BlankValueOk = false
          Description  = ""
]

Query
[
     Name         = "InclueMd"
     Type         = Checkbox
     Label        = "Include content metadata?"
     DefaultValue = false
     Description  = "Include all customer metadata?"
]
]
# This name is significant and identifies this as a Search Criteria Extensions
block.
SearchMdExt
[
   Query
[
     Name         = "CaseName"
     Type         = String
     Label        = "Case Name"
     DefaultValue = ""
     BlankValueOk = true
     Description  = "What is the name of the case?"
]

Query
[
     Name         = "AgentName"
     Type         = Choice
     Label        = "Agent Name"
          BlankValueOk = true
     Description  = "What is the Agent's name?"
     Choice       = "John Napoli"
     Choice       = "Katie Aguilar"
     Choice       = "Justin Campbell"
          EditableChoice = true
]

Query
[
     Name         = "AgentId"
     Type         = Spin
     Label        = "Agent ID"
     DefaultValue = 1001
```

© 2015

```
    Description  = "The ID number of the agent."
    LowerLimit   = 1000
    UpperLimit   = 5000
]

Query
[
    Name         = "CaseType"
    Type         = Choice
    Label        = "Case Type"
    Description  = "What is the case type?"
    Choice       = "Arson"
    Choice       = "Theft"
    Choice       = "Narcotics"
]

Query
[
         Name         = "A Pathname"
         Type         = Pathname
         Label        = "Pathname"
         DefaultValue = ""
         BlankValueOk = false
         Description  = ""
]

Query
[
    Name         = "InclueMd"
    Type         = Checkbox
    Label        = "Include content metadata?"
    DefaultValue = false
    Description  = "Include all customer metadata?"
]
]
```

## Site.cfg

Use a Site.cfg file to work remotely on a network subnet that does not have multicast capabilities. Not having multicast will prevent the Phoenix RSM Locator Service on your local client machine from seeing vaults in Vault Admin, viewing cameras in the Live Viewer, and from viewing search results in Surveillance Video Manager. This capability is intended only for advanced users.

- Create a Site.cfg using any text editor and save as a plain text document. Once created, it needs to be added to the following path: <install-dir>\Config.

© 2015

- Site.cfg is a block structured text file. At the end of this section, there is a sample Site.cfg. You will need to modify the file to meet your own criteria before implementing it.

Site.cfg is comprised of at least one or more policy_name blocks, each is for a remote site.

- The policy_name field is for information use. It can be set to anything but it must exist.
- The version and type fields must be set as shown in the table below.
- You can place as many remote site blocks into the file as you need.

Everything is case sensitive, including the filename (Site.cfg).

| Block name | Valid Token/Values | Description |
|---|---|---|
| **policy_name = "<*policy name*>"** | version = "1.0" | The value for version must be set to "1.0".<br><br>Required |
| | type = "sitecfg" | The value for type must be set to "sitecfg".<br><br>Required. |
| | ip_address = "<*IP address*>" | The IP address for the remote site that you are trying to access.<br><br>Required. |
| | description = "<*character string*>" | The label for the control as it will appear in the application.<br><br>Valid values = a string<br><br>Required. |

## Create a Site.cfg - Example

1. Open a text editor, such as WordPad or Notepad, and start a new document. If using WordPad, be sure to create a Text Document (.txt) and not Rich Text Format (.rtf).
2. Copy and paste the following Site.cfg sample file into the new document.

```
policy_name = "DSM-NVR"
[
        version          = "1.0"
        type             = "sitecfg"
        ip_address       = "172.16.42.28"
        description      = "DSM-NVR"
]
```

© 2015

```
policy_name = "IC-NVR"
[
        version          = "1.0"
        type             = "sitecfg"
        ip_address       = "172.16.153.18"
        description      = "IC-NVR"
]

policy_name = "QC-NVR"
[
        version          = "1.0"
        type             = "sitecfg"
        ip_address       = "172.16.138.18"
        description      = "QC-NVR"
]

policy_name = "WL-NVR"
[
        version          = "1.0"
        type             = "sitecfg"
        ip_address       = "172.16.90.18"
        description      = "WL-NVR"
]
```

3. Save the document to <install-dir>/Config, naming it **Site.cfg**.
4. Launch your Phoenix RSM Vault Admin, Live Viewer, or Surveillance Video Manager.
5. While the splash screen is being displayed, a **Remote Site** dialog box will pop-up and be displayed. Choose your remote site from the drop-down list.
    - **Local Network** is a default choice and is always available.
6. Click **OK** to continue opening your application.

Once this file is created, you can go back and modify it at any time with different or additional policy names for remote sites. See the above sections for tokens/values to change.

## Key Configurations

Phoenix RSM enables you to use special settings to modify its default functionality. These settings are called "keys." It is important to note that a Windows operating system uses keys differently than a Linux or Mac operating system.

- Windows 32-bit - Keys for customizing functionality are located in the Registry at <Local Machine>\Software\SoleraTec\Phoenix.
- Windows 64-bit - Keys for customizing functionality are located in the Registry at <Local Machine>\Software\Wow6432Node\SoleraTec\Phoenix.
- Linux - A file at /etc/SoleraTec/Keys.conf is created when it is installed.
- Mac - A file at /Applications/SoleraTec/Keys.conf is created when it is installed.

© 2015

## Keys.conf File Format (Linux and Mac Only)

- One key per line.
- Line is terminated by a new line character <NEWLINE> or end of file <EOF>.
- Fields in line are delimited by <TAB> or <SPACE>.

### Keys.conf Line Format

**<Name>**<TAB>**<Type>**<TAB>**<Length>**<TAB>**<Value>[\n,EOF]**

- **<Name>** is limited to 1024 characters.
- **<Type>** As specified in table below.
- **<Length>** As specified in table below.
- **<Value>** format depends on the type of data:
  - **Char:** The value is read as a character string.
  - **Int32:** The value is read as a 32 bit signed integer.
  - **Binary:** The value is read as a series of bytes with each byte represented by a hex pair with a single space between each byte.

### Keys.conf Line Format Examples

- key_name_1<TAB>Char<TAB>18<TAB>this is a char key<NEWLINE>
- key_name_2<SPACE>Int32<SPACE>4<SPACE>1234<NEWLINE>
- key_name_4<TAB>Binary<TAB>14<TAB>1a 2e f1 20 9d<EOF>

## Keys

By default, only the **InstallRoot** key is included when Phoenix RSM is installed.

| Key |
| --- |
| **Name:** CameraCacheDir<br>**Description:** Specifies a location where Phoenix RSM applications may store temporary video captured directly from cameras.<br>**Default:** |

© 2015

| Key |
| --- |
| <Product Installation Directory>/VideoCache<br><br>**Used by:** All Phoenix RSM Extension applications<br><br>**Windows Registry Settings:**<br><br>**Key Type:** String value<br><br>**Value:** Pathname of directory<br><br>**Keys.conf Format:**<br><br>**Type:** Char<br><br>**Length:** Number of characters in Value<br><br>**Value:** Pathname of directory<br><br>**Sample Usage:** CameraCacheDir Char 13 C:/VideoCache |
| **Name:** CCExtractorPathname<br><br>**Description:** Pathname of the executable used to extract closed caption data from video.<br><br>**Default:**<br><br>Windows: <Product Installation Directory>\Bin\CCExtractor.exe<br><br>Non-Windows: <Product Installation Directory>/Bin/CCExtractor<br><br>**Used by:** Target and Process<br><br>**Windows Registry Settings:**<br><br>**Key Type:** String value<br><br>**Value:** Pathname of executable<br><br>**Keys.conf Format:**<br><br>**Type:** Char<br><br>**Length:** Number of characters in Value<br><br>**Value:** Pathname of executable<br><br>**Sample Usage:** CCExtractorPathname Char 14 C:/MyExtractor |
| **Name:** CntMaxTermsPerDoc<br><br>**Description:** Specifies the maximum number of terms that will be scanned for content keyword generation in a single file.<br><br>**Default:** 10485760 |

© 2015

| Key |
| --- |
| **Used by:** Vault<br>**Windows Registry Settings:**<br>**Key Type:** DWORD value<br>**Value:** Limit in number of terms<br>**Keys.conf Format:**<br>**Type:** Int32<br>**Length:** 4<br>**Value:** Limit in number of terms<br>**Sample Usage:** CntMaxTermsPerDoc Int32 4 5000 |
| **Name:** CntTextExtList<br>**Description:** Specifies which files will be considered text files and thus scanned for content.<br>**Default:** doc;txt;cfg;cpp;c;cc;cxx;h;dsw;exc;hpp;rtf;htm;html;hxx;log;mk;ppt;rc;sln;vbvbs;bat;xls;xml;sh;cshrc;shrc<br>**Used by:** Vault<br>**Windows Registry Settings:**<br>**Key Type:** String value<br>**Value:**<br><text extension list>: <text extension>[SEMI-COLON <text extension>]*<br><text extension>: <string of characters><br>**Keys.conf Format:**<br>**Type:** Char<br>**Length:** Number of characters in Value<br>**Value:**<br><text extension list>: <text extension>[SEMI-COLON <text extension>]*<br><text extension>: <string of characters><br>**Sample Usage:** CntTextExtList Char 11 doc;bat;cpp |
| **Name:** CntTermsLimit<br>**Description:** Specifies the amount of a file scanned for content keyword generation. |

© 2015

| Key |
| --- |
| **Default:** 10485760<br>**Used by:** Vault<br>**Windows Registry Settings:**<br>**Key Type:** DWORD value<br>**Value:** Limit in bytes<br>**Keys.conf Format:**<br>**Type:** Int32<br>**Length:** 4<br>**Value:** Limit in bytes<br>**Sample Usage:** CntTermsLimit Int32 4 1024 |
| **Name:** DataServicesSvcPriority<br>**Description:** Set process priority of DataServicesSvc.<br>**Default:** standard<br>**Used by:** DataServicesSvc<br>**Windows Registry Settings:**<br>**Key Type:** String Value<br>**Value:** low, standard, high<br>**Keys.conf Format:**<br>**Type:** Char<br>**Length:** Number of characters in Value<br>**Value:** low, standard, high<br>**Sample Usage:** DataServicesSvcPriority Char 4 high |
| **Name:** DbSyncIntOps<br>**Description:** Number of operations between syncing database to disk. A value of zero will disable all sync operations.<br>**Default:** 10000<br>**Used by:** VaultSvc<br>**Windows Registry Settings:** |

© 2015

| Key |
| --- |
| **Key Type:** DWORD value<br>**Value:** Number of operations<br>**Keys.conf Format:**<br>**Type:** Int32<br>**Length:** 4<br>**Value:** Number of operations<br>**Sample Usage:** DbSyncIntOps Int32 4 10246 |
| **Name:** DoBroadcast<br>**Description:** Enable broadcast of events and messages such as location of Vaults and Vault startup/shutdown.<br>**Default:** 1 (true)<br>**Used by:** VaultSvc, TgtProcSvc, LocSvc<br>**Windows Registry Settings:**<br>**Key Type:** DWORD value<br>**Value:** 0 (false) or 1 (true)<br>**Keys.conf Format:**<br>**Type:** Int32<br>**Length:** 4<br>**Value:** 0 (false) or 1 (true)<br>**Sample Usage:** DoBroadcast Int32 4 1 |
| **Name:** DoMulticast<br>**Description:** Enable multicast of events and messages such as location of Vaults and Vault startup/shutdown.<br>**Default:** 1 (true)<br>**Used by:** VaultSvc, TgtProcSvc, LocSvc<br>**Windows Registry Settings:**<br>**Key Type:** DWORD value<br>**Value:** 0 (false) or 1 (true)<br>**Keys.conf Format:** |

© 2015

| Key |
| --- |
| **Type:** Int32<br>**Length:** 4<br>**Value:** 0 (false) or 1 (true)<br>**Sample Usage:** DoMulticast Int32 4 1 |
| **Name:** FfmbcExePathname<br>**Description:** Pathname to ffmbc executable.<br>**Default:** <install-dir>/Bin/ffmbc.exe<br>**Used by:** VideoComponentsGen<br>**Windows Registry Settings:**<br>**Key Type:** String value<br>**Value:** Pathname of executable<br>**Keys.conf Format:**<br>**Type:** Char<br>**Length:** Number of characters in Value<br>**Value:** Pathname of the executable<br>**Sample Usage:** FfmbcExePathname Char 14 C:/MyFfmbc.exe |
| **Name:** FfmpegExePathname<br>**Description:** Pathname to ffmpeg executable.<br>**Default:** <install-dir>/Bin/ffmpeg.exe<br>**Used by:** VideoComponentsGen<br>**Windows Registry Settings:**<br>**Key Type:** String value<br>**Value:** Pathname of executable<br>**Keys.conf Format:**<br>**Type:** Char<br>**Length:** Number of characters in Value<br>**Value:** Pathname of executable<br>**Sample Usage:** FfmpegExePathname Char 15 C:/MyFfmpeg.exe |

© 2015

| Key |
| --- |
| **Name:** FfmpegJoinExePathname<br>**Description:** Pathname to joining version of ffmpeg executable.<br>**Default:** <install-dir>/Bin/ffmpeg_v112.exe<br>**Used by:** VideoComponentsGen<br>**Windows Registry Settings:**<br>**Key Type:** String value<br>**Value:** Pathname of executable<br>**Keys.conf Format:**<br>**Type:** Char<br>**Length:** Number of characters in Value<br>**Value:** Pathname of executable<br>**Sample Usage:** FfmpegJoinExePathname Char 15 C:/MyJoiner.exe |
| **Name:** InstallRoot<br>**Description:** The location of /Phoenix directory.<br>**Default:** /usr/local/Phoenix<br>**Used by:** All Phoenix RSM applications<br>**Windows Registry Settings:**<br>**Key Type:** String value<br>**Value:** Pathname of the root directory<br>**Keys.conf Format:**<br>**Type:** Char<br>**Length:** Number of characters in Value<br>**Value:** Pathname of the root directory<br>**Sample Usage:** InstallRoot Char 18 /usr/local/Phoenix |
| **Name:** IpAddressList<br>**Description:** Restricts TCP addresses that are used when the computer has multiple network connections.<br>**Default:** Addresses of all network connections |

© 2015

| Key |
| --- |
| **Used by:** All Phoenix RSM applications<br>**Windows Registry Settings:**<br>**Key Type:** String value<br>**Value:**<br><address list>: <address>[COMMA <address>]*<br><address>: <xx.xx.xx.xx>/<mask><br>**Keys.conf Format:**<br>**Type:** Char<br>**Length:** Number of characters in Value<br>**Value:**<br><address list>: <address>[COMMA <address>]*<br><address>: <xx.xx.xx.xx>/<mask><br>**Sample Usage:** lpAddressList Char 40 192.168.1.0/ffffff00,127.0.0.1/ffffff00 |
| **Name:** LfrMaxFileSizeBytes<br>**Description:** Specifies the maximum file size in bytes for log file rotation.<br> Setting a value that is less than the default value could result in slower system operation.<br>**Default:** 10485760 (10MB)<br>**Used by:** All Phoenix RSM applications<br>**Windows Registry Settings:**<br>**Key Type:** DWORD value<br>**Value:** Limit in bytes, greater than zero<br>**Keys.conf Format:**<br>**Type:** Int32<br>**Length:** 4<br>**Value:** Limit in bytes, greater than zero<br>**Sample Usage:** LfrMaxFileSizeBytes Int32 4 10485760 |

© 2015

| Key |
| --- |
| **Name:** LfrMaxNumFiles<br><br>**Description:** Specifies the maximum number of files to keep during log file rotation.<br><br> Setting a value that is less than the default value could result in slower system operation.<br><br>**Default:** 2<br><br>**Used by:** All Phoenix RSM applications<br><br>**Windows Registry Settings:**<br><br>**Key Type:** DWORD value<br><br>**Value:** Limit in number of files, greater than 1<br><br>**Keys.conf Format:**<br><br>**Type:** Int32<br><br>**Length:** 4<br><br>**Value:** Limit in number of files, greater than 1<br><br>**Sample Usage:** LfrMaxNumFiles Int32 4 2 |
| **Name:** LfrCheckIntervalSec<br><br>**Description:** Specifies the check interval in seconds for log file rotation.<br><br> Setting a value that is less than the default value could result in slower system operation.<br><br>**Default:** 3600 (1 hour)<br><br>**Used by:** All Phoenix RSM applications<br><br>**Windows Registry Settings:**<br><br>**Key Type:** DWORD value<br><br>**Value:** Interval in seconds, greater than zero<br><br>**Keys.conf Format:**<br><br>**Type:** Int32<br><br>**Length:** 4<br><br>**Value:** Interval in seconds, greater than zero |

© 2015

| Key |
| --- |
| **Sample Usage:** LfrCheckIntervalSec Int32 4 3600 |
| **Name:** LocSvcPriority<br>**Description:** Set process priority of LocSvc.<br>**Default:** standard<br>**Used by:** LocSvc<br>**Windows Registry Settings:**<br>**Key Type:** String Value<br>**Value:** low, standard, high<br>**Keys.conf Format:**<br>**Type:** Char<br>**Length:** Number of characters in Value<br>**Value:** low, standard, high<br>**Sample Usage:** LocSvcPriority Char 4 high |
| **Name:** MediaPlayerDefaultVolume<br>**Description:** Specifies the initial volume setting when playing video.<br>**Default:** 50<br>**Used by:** Video Content Manager, Surveillance Video Manager, Live Viewer<br>**Windows Registry Settings:**<br>**Key Type:** DWORD value<br>**Value:** Volume, greater than zero<br>**Keys.conf Format:**<br>**Type:** Int32<br>**Length:** 4<br>**Value:** Volume, greater than zero<br>**Sample Usage:** MediaPlayerDefaultVolume Int32 4 50 |
| **Name:** MulticastAddress<br>**Description:** Specifies the multicast address used when various components communicate. |

© 2015

| Key |
| --- |
| **Default:** 224.0.23.160<br><br>**Used by:** All Phoenix RSM applications<br><br>**Windows Registry Settings:**<br><br>**Key Type:** String value<br><br>**Value:** IP address<br><br>**Keys.conf Format:**<br><br>**Type:** Char<br><br>**Length:** Number of characters in Value<br><br>**Value:** IP address<br><br>**Sample Usage:** MulticastAddress Char 12 226.0.19.156 |
| **Name:** MulticastIfcAddress<br><br>**Description:** Indicates which interface on host machine will be used to send out multicast packets:<br><br>• If a complete address is given, the network interface corresponding to that address will be used for sending multicast packets.<br><br>• If an address and mask are specified, the first network interface that matches the non-masked portion of the specified address will be used.<br><br> Using a mask enables a network interface to be specified by network address. Using a mask avoids errors when the network interface changes address through the use of DHCP.<br><br>**Default:** Interface chosen by host machine<br><br>**Used by:** All Phoenix RSM applications<br><br>**Windows Registry Settings:**<br><br>**Key Type:** String value<br><br>**Value:** <xx.xx.xx.xx> or <xx.xx.xx.xx>/<mask><br><br>**Keys.conf Format:**<br><br>**Type:** Char<br><br>**Length:** Number of characters in Value<br><br>**Value:** <xx.xx.xx.xx> or <xx.xx.xx.xx>/<mask> |

© 2015

| Key |
| --- |
| **Sample Usage:** MulticastIfcAddress Char 20 192.168.1.0/ffffff00 |
| **Name:** MulticastTtl<br>**Description:** Specifies the multicast TTL (Time To Live) value.<br>**Default:** 255<br>**Used by:** All Phoenix RSM applications<br>**Windows Registry Settings:**<br>**Key Type:** DWORD value<br>**Value:** TTL value<br>**Keys.conf Format:**<br>**Type:** Int32 in the range of 0 - 255<br>**Length:** 4<br>**Value:** TTL value<br>**Sample Usage:** MulticastTtl Int32 4 10 |
| **Name:** NotifyClearCmd<br>**Description:** Command to execute when clearing an error condition. Used for notification.<br>**Default:** none<br>**Used by:** All Phoenix RSM applications<br>**Windows Registry Settings:**<br>**Key Type:** String value<br>**Value:** Pathname to the batch file<br>**Keys.conf Format:**<br>**Type:** Char<br>**Length:** Number of characters in Value<br>**Value:** Pathname to the batch file<br>**Sample Usage:** NotifyClearCmd Char 27 C:/MyNotificationScript.bat |
| **Name:** NotifySetCmd |

© 2015

| Key |
| --- |
| **Description:** Command to execute when clearing an error condition. Used for notification.<br><br>**Default:** none<br><br>**Used by:** All Phoenix RSM applications<br><br>**Windows Registry Settings:**<br><br>**Key Type:** String value<br><br>**Value:** Pathname to the batch file<br><br>**Keys.conf Format:**<br><br>**Type:** Char<br><br>**Length:** Number of characters in Value<br><br>**Value:** Pathname to the batch file<br><br>**Sample Usage:** NotifySetCmd Char 27 C:/MyNotificationScript.bat |
| **Name:** PictureExtList<br><br>**Description:** Specifies which files will be considered picture files and therefore processed as picture files when option is enabled in Target and Process Policies (if enabled) or manual Target and Process jobs (if enabled).<br><br>**Default:** bmp;gif;jpeg;jpg;pict;pct;png;raw;tif;tiff<br><br>**Used by:** Target and Process, Target and Process Policies, Target and Process Service<br><br>**Windows Registry Settings:**<br><br>**Key Type:** String value<br><br>**Value:**<br><br><picture extension list>: <picture extension>[SEMI-COLON <picture extension>]*<br><br><picture extension>: <string of characters><br><br>**Keys.conf Format:**<br><br>**Type:** Char<br><br>**Length:** Number of characters in picture<br><br>**Value:** |

© 2015

| Key |
| --- |
| <picture extension list>: <picture extension>[SEMI-COLON <picture extension>]*<br><br><picture extension>: <string of characters><br><br>**Sample Usage:** PictureExtList Char 11 bmp;gif;jpg |
| **Name:** PrimaryNicName<br><br>**Description:** Defines the NIC (Network Interface Card) which is used as the primary interface.<br><br>**Default:**<br><br>In Linux, the primary network interface card (NIC) is chosen by looking for the first non-zero IP address, "Up" device eth0, eth1, eth2, ... If none found, then first device as shown in "ifconfig -a".<br><br>Apple is same as Linux except uses device names en0, en1, en2, ...<br><br>Windows is chosen using the first non-zero, "Enabled" NIC in the list shown in the Advanced Settings dialog box in the Network Connections window. Open Network Connections and Advanced Settings option in the Advanced menu.<br><br>In all cases above, the Local Loopback device is only chosen if no other device is available.<br><br>**Used by:** All Phoenix RSM applications.<br><br>**Windows Registry Settings:**<br><br>**Key Type:** String value<br><br>**Value:** Network Interface Description<br><br>**Keys.conf Format:**<br><br>**Type:** Char<br><br>**Length:** Number of characters in value<br><br>**Value:** Network Interface Name<br><br>**Sample Usage:** PrimaryNicName Char 4 eth0 |
| **Name:** RccMinVideoSizeBytes<br><br>**Description:** Minimum size that a RTSP recorded video file must have to be considered valid, in bytes.<br><br>**Default:** 10240<br><br>**Used by:** TgtProcSvc |

© 2015

| Key |
| --- |
| **Windows Registry Settings:**<br>**Key Type:** DWORD<br>**Value:** Size in bytes<br>**Keys.conf Format:**<br>**Type:** Int32<br>**Length:** 4<br>**Value:** Size in bytes<br>**Sample Usage:** RccMinVideoSizeBytes Int32 4 8192 |
| **Name:** RestrictedPortsList<br>**Description:** Restricts TCP port usage to a set or range.<br>**Default:** Use all ports<br>**Used by:** All Phoenix RSM applications<br>**Windows Registry Settings:**<br>**Key Type:** String value<br>**Value:**<br><ranges>: <range> [COMMA <range>]*<br><range>: <port-low> HYPHEN <port-high><br>**Keys.conf Format:**<br>**Type:** Char<br>**Length:** Number of characters in Value<br>**Value:**<br><ranges>: <range> [COMMA <range>]*<br><range>: <port-low> HYPHEN <port-high><br>**Sample Usage:** RestrictedPortsList Char 20 5000-5110,5500-5521 |
| **Name:** SarAdvancedFeaturesEnable<br>**Description:** Enables metadata editing, file grouping, file purging, and file protection settings editing via Search and Retrieve.<br>**Default:** 0 (disabled) |

© 2015

| Key |
| --- |
| **Used by:** Search and Retrieve<br>**Windows Registry Settings:**<br>**Key Type:** DWORD value<br>**Value:** 0 (disabled) or 1 (enabled)<br>**Keys.conf Format:**<br>**Type:** Int32<br>**Length:** 4<br>**Value:** 0 (disabled) or 1 (enabled)<br>**Sample Usage:** SarAdvancedFeaturesEnable Int32 4 1 |
| **Name:** SarNoDelFilesInSearch<br>**Description:** When set to "1" for either host or user, it will not allow the user to make the choice to include deleted files in their searches.<br>**Default:** 0 (disabled)<br>**Used by:** Search and Retrieve<br>**Windows Registry Settings:**<br>**Key Type:** DWORD value<br>**Value:** 0 (disabled) or 1 (enabled)<br>**Keys.conf Format:**<br>**Type:** Int32<br>**Length:** 4<br>**Value:** 0 (disabled) or 1 (enabled)<br>**Sample Usage:** SarNoDelFilesInSearch Int32 4 1 |
| **Name:** SarPurgeFeatureEnable<br>**Description:** When set to "1" for either host or user, it will allow the user to use the Purge functionality in Search and Retrieve.<br>**Default:** 0 (disabled)<br>**Used by:** Search and Retrieve<br>**Windows Registry Settings:**<br>**Key Type:** DWORD value |

© 2015

| Key |
| --- |
| **Value:** 0 (disabled) or 1 (enabled)<br>**Keys.conf Format:**<br>**Type:** Int32<br>**Length:** 4<br>**Value:** 0 (disabled) or 1 (enabled)<br>**Sample Usage:** SarPurgeFeatureEnable Int32 4 1 |
| **Name:** TapeFsGetIntSec<br>**Description:** Interval in seconds at which a tape drive is queried for remaining free space on the current tape. Minimum is 2 seconds.<br>**Default:** 10<br>**Used by:** VaultSvc<br>**Windows Registry Settings:**<br>**Key Type:** DWORD value<br>**Value:** Interval in seconds, greater than or equal to 2<br>**Keys.conf Format:**<br>**Type:** Int32<br>**Length:** 4<br>**Value:** Interval in seconds, greater than or equal to 2<br>**Sample Usage:** TapeFsGetIntSec Int32 4 10 |
| **Name:** TapeMinBlockSizeKB<br>**Description:** Sets the minimum block size for data written to tape.<br>**Default:** 48<br>**Used by:** VaultSvc<br>**Windows Registry Settings:**<br>**Key Type:** DWORD value<br>**Value:** Block size<br>**Keys.conf Format:**<br>**Type:** Int32 |

© 2015

| Key |
| --- |
| **Length:** 4<br><br>**Value:** Block size<br><br>**Sample Usage:** TapeMinBlockSizeKB Int32 4 48 |
| **Name:** TapUseHardLink<br><br>**Description:** Specifies the use of hard links and applies only to "move" operations where the camera cache is located on the same file system as the destination storage media.<br><br>**Default:** 0 (false)<br><br>**Used by:** TgtProcSvc<br><br>**Windows Registry Settings:**<br><br>**Key Type:** DWORD value<br><br>**Value:** 0 (false) or 1 (true)<br><br>**Keys.conf Format:**<br><br>**Type:** Int32<br><br>**Length:** 4<br><br>**Value:** 0 (false) or 1 (true)<br><br>**Sample Usage:** TapUseHardLink Int32 4 1 |
| **Name:** TapVideoCaptureWriteBufferSizeKB<br><br>**Description:** Sets the video capture write buffer size in kilobytes. If zero, then use system buffer setting.<br><br>**Default:** 0<br><br>**Used by:** TgtProcSvc<br><br>**Windows Registry Settings:**<br><br>**Key Type:** DWORD value<br><br>**Value:** Minimum of 0<br><br>**Keys.conf Format:**<br><br>**Type:** Int32<br><br>**Length:** 4<br><br>**Value:** Minimum of 0 |

© 2015

| Key |
| --- |
| **Sample Usage:** TapVideoCaptureWriteBufferSizeKB Int32 4 0 |
| **Name:** TempDir<br>**Description:** Specifies a location where Phoenix RSM applications may store temporary files.<br>**Default:**<br>Windows: Documents and Settings/<user>/Local Settings/Temp<br>Non-Windows: /tmp<br>**Used by:** All Phoenix RSM applications<br>**Windows Registry Settings:**<br>**Key Type:** String value<br>**Value:** Pathname of directory<br>**Keys.conf Format:**<br>**Type:** Char<br>**Length:** Number of characters in Value<br>**Value:** Pathname of directory<br>**Sample Usage:** TempDir Char 7 C:/tmp |
| **Name:** TgtProcSvcPriority<br>**Description:** Set process priority of TgtProcSvc.<br>**Default:** standard<br>**Used by:** TgtProcSvc<br>**Windows Registry Settings:**<br>**Key Type:** String Value<br>**Value:** low, standard, high<br>**Keys.conf Format:**<br>**Type:** Char<br>**Length:** Number of characters in Value<br>**Value:** low, standard, high<br>**Sample Usage:** TgtProcSvcPriority Char 4 high |

© 2015

| Key |
| --- |
| **Name:** VaultSvcPriority<br>**Description:** Set process priority of VaultSvc.<br>**Default:** standard<br>**Used by:** VaultSvc<br>**Windows Registry Settings:**<br>**Key Type:** String Value<br>**Value:** low, standard, high<br>**Keys.conf Format:**<br>**Type:** Char<br>**Length:** Number of characters in Value<br>**Value:** low, standard, high<br>**Sample Usage:** VaultSvcPriority Char 4 high |
| **Name:** VideoClipGenPathname<br>**Description:** Pathname of executable to create a clip of a video file.<br>**Default:** <install-dir>/Bin/VideoComponentsGen.exe<br>**Used by:** VaultSvc<br>**Windows Registry Settings:**<br>**Key Type:** String value<br>**Value:** Pathname of executable<br>**Keys.conf Format:**<br>**Type:** Char<br>**Length:** Number of characters in Value<br>**Value:** Pathname of executable<br>**Sample Usage:** VideoClipGenPathname Char 16 C:/MyClipper.exe |
| **Name:** VideoComponentsGenBackend<br>**Description:** VideoComponentsGen's backend package to use.<br>**Default:** ffmpeg |

© 2015

| Key |
| --- |
| **Used by:** Target and Process, TgtProcSvc, Video Content Manager, Surveillance Video Manager<br><br>**Windows Registry Settings:**<br><br>**Key Type:** String value<br><br>**Value:** ffmpeg<br><br>**Keys.conf Format:**<br><br>**Type:** Char<br><br>**Length:** Number of characters in Value<br><br>**Value:** ffmpeg<br><br>**Sample Usage:** VideoComponentsGenBackend Char 6 ffmpeg |
| **Name:** VideoComponentsGenMaxInstances<br><br>**Description:** The number of transcoding processes that can be run simultaneously. It can be represented in several different formats:<br><br>= : Use the number of cores (default)<br>0 : Unlimited<br>n : Use this number explicitly<br>*n : Multiply the number of cores by n<br>/n : Divide the number of cores by n<br>+n : Add n to the number of cores<br>-n : Subtract n from the number of cores<br><br>**Default:** =<br><br>**Used by:** Target and Process, TgtProcSvc, Video Content Manager, Surveillance Video Manager<br><br>**Windows Registry Settings:**<br><br>**Key Type:** String value<br><br>**Value:** Number of transcoding processes<br><br>**Keys.conf Format:**<br><br>**Type:** Char<br><br>**Length:** Number of characters in Value<br><br>**Value:** Number of transcoding processes<br><br>**Sample Usage:** VideoComponentsGenMaxInstances Char 2 +6 |
| **Name:** VideoComponentsGenMaxThreads |

© 2015

| Key |
| --- |
| **Description:** The number of threads that can be used by each transcoding process. A value of 0 (default) indicates that the number of threads will not be restricted but will instead be left to the transcoding engine.<br><br>**Default:** 0<br><br>**Used by:** Target and Process, TgtProcSvc, Video Content Manager, Surveillance Video Manager<br><br>**Windows Registry Settings:**<br><br>**Key Type:** DWORD value<br><br>**Value:** Minimum of 0<br><br>**Keys.conf Format:**<br><br>**Type:** Int32<br><br>**Length:** 4<br><br>**Value:** Minimum of 0<br><br>**Sample Usage:** VideoComponentsGenMaxThreads Int32 4 0 |
| **Name:** VideoComponentsGenPathname<br><br>**Description:** Pathname of executable to create a thumbnail or low res proxy.<br><br>**Default:** <install-dir>/Bin/VideoComponentsGen.exe<br><br>**Used by:** Target and Process, TgtProcSvc, Video Content Manager, Surveillance Video Manager<br><br>**Windows Registry Settings:**<br><br>**Key Type:** String value<br><br>**Value:** Pathname to executable<br><br>**Keys.conf Format:**<br><br>**Type:** Char<br><br>**Length:** Number of characters in Value<br><br>**Value:** Pathname to executable<br><br>**Sample Usage:** VideoComponentsGenPathname Char 17 C:/MyVideoGen.exe |
| **Name:** VideoComponentsGenPictWidthLow<br><br>**Description:** Specifies the picture thumbnail target width, in pixels, for the low quality setting. |

© 2015

| Key |
| --- |
| **Default:** 100<br>**Used by:** Target and Process Service<br>**Windows Registry Settings:**<br>**Key Type:** DWORD value<br>**Value:** Minimum of 1<br>**Keys.conf Format:**<br>**Type:** Int32<br>**Length:** 4<br>**Value:** Minimum of 1<br>**Sample Usage:** VideoComponentsGenPictWidthLow Int32 4 200 |
| **Name:** VideoComponentsGenPictHeightLow<br>**Description:** Specifies the picture thumbnail target height, in pixels, for the low quality setting.<br>**Default:** 100<br>**Used by:** Target and Process Service<br>**Windows Registry Settings:**<br>**Key Type:** DWORD value<br>**Value:** Minimum of 1<br>**Keys.conf Format:**<br>**Type:** Int32<br>**Length:** 4<br>**Value:** Minimum of 1<br>**Sample Usage:** VideoComponentsGenPictHeightLow Int32 4 200 |
| **Name:** VideoComponentsGenPictQualLow<br>**Description:** Specifies the picture thumbnail image quality for the low quality setting.<br>**Default:** 2<br>**Used by:** Target and Process Service<br>**Windows Registry Settings:** |

© 2015

| Key |
| --- |
| **Key Type:** DWORD value<br>**Value:** 1 (worst) – 10 (best)<br>**Keys.conf Format:**<br>**Type:** Int32<br>**Length:** 4<br>**Value:** 1 (worst) – 10 (best)<br>**Sample Usage:** VideoComponentsGenPictQualLow Int32 4 3 |
| **Name:** VideoComponentsGenPictWidthMed<br>**Description:** Specifies the picture thumbnail target width, in pixels, for the medium quality setting.<br>**Default:** 320<br>**Used by:** Target and Process Service<br>**Windows Registry Settings:**<br>**Key Type:** DWORD value<br>**Value:** Minimum of 1<br>**Keys.conf Format:**<br>**Type:** Int32<br>**Length:** 4<br>**Value:** Minimum of 1<br>**Sample Usage:** VideoComponentsGenPictWidthMed Int32 4 400 |
| **Name:** VideoComponentsGenPictHeightMed<br>**Description:** Specifies the picture thumbnail target height, in pixels, for the medium quality setting.<br>**Default:** 240<br>**Used by:** Target and Process Service<br>**Windows Registry Settings:**<br>**Key Type:** DWORD value<br>**Value:** Minimum of 1<br>**Keys.conf Format:** |

© 2015

| Key |
| --- |
| **Type:** Int32<br>**Length:** 4<br>**Value:** Minimum of 1<br>**Sample Usage:** VideoComponentsGenPictHeightMed Int32 4 400 |
| **Name:** VideoComponentsGenPictQualMed<br>**Description:** Specifies the picture thumbnail image quality for the medium quality setting.<br>**Default:** 5<br>**Used by:** Target and Process Service<br>**Windows Registry Settings:**<br>**Key Type:** DWORD value<br>**Value:** 1 (worst) – 10 (best)<br>**Keys.conf Format:**<br>**Type:** Int32<br>**Length:** 4<br>**Value:** 1 (worst) – 10 (best)<br>**Sample Usage:** VideoComponentsGenPictQualMed Int32 4 3 |
| **Name:** VideoComponentsGenPictWidthHigh<br>**Description:** Specifies the picture thumbnail target width, in pixels, for the high quality setting.<br>**Default:** Original picture width<br>**Used by:** Target and Process Service<br>**Windows Registry Settings:**<br>**Key Type:** DWORD value<br>**Value:** Minimum of 1<br>**Keys.conf Format:**<br>**Type:** Int32<br>**Length:** 4<br>**Value:** Minimum of 1 |

© 2015

| Key |
| --- |
| **Sample Usage:** VideoComponentsGenPictWidthHigh Int32 4 600 |
| **Name:** VideoComponentsGenPictHeightHigh<br>**Description:** Specifies the picture thumbnail target height, in pixels, for the high quality setting.<br>**Default:** Original picture height<br>**Used by:** Target and Process Service<br>**Windows Registry Settings:**<br>**Key Type:** DWORD value<br>**Value:** Minimum of 1<br>**Keys.conf Format:**<br>**Type:** Int32<br>**Length:** 4<br>**Value:** Minimum of 1<br>**Sample Usage:** VideoComponentsGenPictHeightHigh Int32 4 600 |
| **Name:** VideoComponentsGenPictQualHigh<br>**Description:** Specifies the picture thumbnail image quality for the high quality setting.<br>**Default:** 7<br>**Used by:** Target and Process Service<br>**Windows Registry Settings:**<br>**Key Type:** DWORD value<br>**Value:** 1 (worst) – 10 (best)<br>**Keys.conf Format:**<br>**Type:** Int32<br>**Length:** 4<br>**Value:** 1 (worst) – 10 (best)<br>**Sample Usage:** VideoComponentsGenPictQualHigh Int32 4 3 |
| **Name:** VideoComponentsGenPriority<br>**Description:** Set process priority of VideoComponentsGen. |

© 2015

| Key |
| --- |
| **Default:** standard<br><br>**Used by:** VideoComponentsGen<br><br>**Windows Registry Settings:**<br><br>**Key Type:** String Value<br><br>**Value:** low, standard, high<br><br>**Keys.conf Format:**<br><br>**Type:** Char<br><br>**Length:** Number of characters in Value<br><br>**Value:** low, standard, high<br><br>**Sample Usage:** VideoComponentsGenPriority Char 4 high |
| **Name:** VideoExtList<br><br>**Description:** Specifies which files will be considered video files and therefore processed as video files when option is enabled in Camera policies (if enabled).<br><br>**Default:** 3g2;3gp;avi;divx;f4v;fbr;flv;m4v;mkv;mov;mp4;mpg;mpg2;mts;mxf;qt;rm;swf;vob;wmv;xvid<br><br>**Used by:** Target and Process Service<br><br>**Windows Registry Settings:**<br><br>**Key Type:** String value<br><br>**Value:**<br><br><video extension list>: <video extension>[SEMI-COLON <video extension>]*<br><br><video extension>: <string of characters><br><br>**Keys.conf Format:**<br><br>**Type:** Char<br><br>**Length:** Number of characters in Value<br><br>**Value:**<br><br><video extension list>: <video extension>[SEMI-COLON <video extension>]*<br><br><video extension>: <string of characters><br><br>**Sample Usage:** VideoExtList Char 11 mpg;mxf;mov |
| **Name:** VltPrefetchQueLen |

© 2015

| Key |
| --- |
| **Description:** Sets the limit for the number of 128K blocks which are initially read from a file when opened for transfer. This value will be reduced if the file is smaller or the device cache size is smaller.<br><br>**Default:** 10<br><br>**Used by:** Vault Service<br><br>**Windows Registry Settings:**<br><br>**Key Type:** DWORD value<br><br>**Value:** Number of 128K blocks initially read<br><br>**Keys.conf Format:**<br><br>**Type:** Int32<br><br>**Length:** 4<br><br>**Value:** Number of 128K blocks initially read<br><br>**Sample Usage:** VltPrefetchQueLen Int32 4 10 |

# Command Line Arguments

The command line arguments are intended for advanced users of Phoenix RSM. Use the command line interface only if you are familiar with command line environments, otherwise, use a Phoenix RSM application.

In Phoenix RSM, command line refers to command line interpreter based Phoenix RSM applications or the line in a command line interpreter where you can type commands. The command line applications provide an alternative way for executing functionality for Phoenix RSM applications.

There are distinct ways to use command line utilities:

- There are several command line executables for desktop client components available with your suite of product applications - for example, VaultAdminCl.exe. These executables with the "Cl" included at the end of the name are completely interactive and offer another way to execute an application's default functionality. This is useful if you have scripts to run or diagnostics work to do. At the command line prompt, if you type **help**, a list of commands appear for you to interact with the application.

  For more information see Locator Admin Command Line, Vault Admin Command Line, and Data Services Command Line.

- Some server components are service applications that run behind the scenes and can be accessed through command line arguments. An advanced user could modify these to allow for additional options to run with the services (other than defaults), or to perform diagnostics on the program. To see a list of available options for a command line utility, use **<executable name> -usage** at the command line prompt.

© 2015

For more information see Vault Service and Data Services Service. Also see the Live Viewer Command Line arguments to open the Live Viewer with customized defaults.

# Locator Admin Command Line

The LocAdminCl keeps track of resources, such as Vaults, in the Information Repository.

- Access **LocAdminCl** from your suite of application products.

## Command Line Options

As needed, append the following options to the application execution path. You can enter a single option, a single option and -usage or -version, or a combination of several options and -usage or -version.

The command line is formed as follows:

```
LocAdminCl <option> <option> . . .
```

- **-input_pathname <pathname>** - Contains the input list of commands.
- **-output_pathname <pathname>** - Define the path to the file containing the output results.
- **-usage** - List all valid parameters.
- **-version** - Display the current version information.

## Interactive Commands and their Arguments

After starting the application, you can enter the following arguments at the prompt.

| Argument | Description |
|---|---|
| advanced <*boolean*> | Set or view advanced mode setting.<br>Valid values = on \| off<br>Default = off |
| broadcast | Register a test entry by broadcast in all global maps. Available only in advanced mode. |
| find <*seconds*> | Find all Locator Services on network and determine how long to wait for responses from other Locator Services on the network.<br>Valid Values = 1 - ∞ |
| format <*alpha*> | Set or view address format. |

© 2015

| Argument | Description |
|---|---|
| | Valid values =<br>• dot<br>• host<br>• full |
| help \| ? | Print usage information for all commands. |
| host <*hostname*> | Set or view default host setting. |
| list <*hostname*> | List entries in locator at <hostname<. In advanced mode, displays extended output. |
| quit | Exit the application. |
| register <*hostname*> | Register a test entry in global map at <hostname>. Appears only in advanced mode. |
| shut <*hostname*> | Shuts down the Locator Service at <hostname>. Available only in advanced mode. |
| status | Print current settings. |
| timeout <*number*> | Set or view communications timeout value.<br>Valid values = 0 - 9. |

For more information see Vault Management, Command Line Arguments, and Locator Service.

## Locator Service

The Locator Service makes dynamic resource allocation possible in Phoenix RSM, which delivers unlimited storage resource accessibility within the network. It is the tool which locates and provides communication between clients and Vaults, enabling them to work like a traditional client/server system but without the need for hard-coded static links between clients and servers. In contrast, the Locator architecture is flexible to allow dynamic client access to any storage resource on your network.

The Locator maintains a list of currently available Phoenix RSM services, by using a multicast and beacon technology, and it provides this list to clients on the network as needed. To accomplish this, the Locator constantly "listens" for active registered Vaults. The Locator list notes Vault status and location changes. Every Locator is self-propagating and shares information with other Locators within the Information Repository.

For more information see Command Line Arguments.

© 2015

# Vault Admin Command Line

Use VaultAdminCl to manage media and Vaults in your Information Repository.

To execute Vault Admin tasks, ensure that the folder where Phoenix RSM is installed is in your command path, open a command prompt, and run VaultAdminCl at the command line. As needed, use the commands listed below. For more information see Vault Admin and Command Line Arguments.

- Access **VaultAdminCl** from your suite of application products.

## Command Line Options

As needed, append the following options to the execution path. When you run VaultAdminCl, the command line is formed as follows:

```
VaultAdminCl <option>
```

- **-input_pathname <pathname>** - Contains the input list of commands.
- **-output_pathname <pathname>** - Define the path to the file containing the output results.
- **-usage** - List all valid parameters.
- **-version** - Display the current version information.

## Interactive Commands and their Arguments

After starting the application, type the following arguments to the command line prompt one at a time. When entering arguments, you can simultaneously enter required variables or enter just a given argument and wait for the system to prompt you for its required variables.

| Argument | Description |
|---|---|
| clist | List all current clients for the selected Vault. |
| close | Close the connection to the selected Vault. |
| diag | Set the diagnostic mode for the selected Vault. |
| drives | List drives for selected Vault. |
| dstat <*drive name*> | Display information about a selected drive. If the name is not listed on the command line, it asks to provide the name. |
| errorlog <*pathname*> | Set the Vault's error log path.<br>Valid values: |

© 2015

| Argument | Description |
|---|---|
| | • pathname - New error log path. |
| format <*notation type*> | Set the current client address format.<br>Valid notations:<br>• dot - Client computer network address is displayed.<br>• host - Client computer name is displayed along with domain and subnet names.<br>• full - Client's host name and port number are displayed. |
| help \| ? | Show valid usages for commands. Use only one command at a time. |
| license <*pathname*> | Set the path for Information Repository license.<br>Valid values:<br>• pathname - New path name to the license file. |
| load <*argument*> | Load the media for the selected Vault.<br>Arguments for a tape Vault with a mailslot:<br>• load from mailslot? <yes \| no><br>• if loading from mailslot, mailslot loc<br>• if not loading from mailslot, storage loc<br>• force reindex of media? <yes \| no><br>Arguments for a tape Vault with no mailslot:<br>• storage loc<br>• force reindex of media? <yes \| no><br>Arguments for a hard disk Vault:<br>• media name<br>• media in default location? <yes \| no><br>• if not in a default location, pathname<br>• force reindex of media? <yes \| no> |
| media | List the media for the selected Vault. |

© 2015

| Argument | Description |
|---|---|
| mstat <*name*> | Display media status.<br>• name - Name of the media to display. |
| name <*name*> | Set the name for the selected Vault.<br>Valid values:<br>• name – New name for the Vault. |
| prepare <*arguments*> | Prepare media for the selected Vault.<br>Arguments for a tape Vault with a mailslot:<br>• media name<br>• Barcode/ID<br>• description<br>• storage pool<br>• content searching <yes \| no><br>• file de-duplication <yes \| no><br>• load from mailslot? <yes \| no><br>  • if loading from mailslot, mailslot loc<br>  • if not loading from mailslot, storage loc<br>• prepare media now? <yes \| no><br>Arguments for a tape Vault with no mailslot:<br>• media name<br>• Barcode/ID<br>• description<br>• storage pool<br>• content searching<br>• file de-duplication<br>• storage loc<br>• prepare media now? <yes \| no><br>Arguments for a hard disk Vault:<br>• media name |

© 2015

| Argument | Description |
|---|---|
| | • description<br>• storage pool<br>• media size<br>• content searching<br>• file de-duplication<br>• store media in default location? <yes \| no><br>• if not in default location, pathname<br>• prepare media now? <yes \| no> |
| quit | Exit the application. |
| reload <*arguments*> | Reload media for the selected Vault.<br>Valid arguments:<br>• media name<br>• force reindex of media? <yes \| no> |
| secure <*boolean*> | Secure/unsecure the selected Vault from any media eject or load commands. You must have administrator rights to execute this command.<br>Valid values:<br>• on<br>• off |
| select <*Vault name*> | Select the Vault for operation. |
| shut <*type of shutdown*> | Close the selected Vault. You must have administrator access to execute this command.<br>Valid values:<br>• extended - Close the Vault after all clients and callbacks have been serviced. Close all open databases.<br>• normal - Close the Vault and all current connections.<br>• restart - Execute a normal shutdown and then restart the Vault. |

© 2015

| Argument | Description |
|---|---|
| | • emergency - Close the Vault immediately. |
| stat | Display status information of selected Vault. |
| timeout <*number*> | Set the communication timeout value.<br>Valid values:<br>• 0 - 10 (where "0" is the shortest, "9" is the longest, and "10" is never.) |
| unload <*arguments*> | Unload media for the selected Vault.<br>Valid arguments:<br>• media name<br>• media tracking? <yes \| no><br>• if keeping track, enter storage location<br>• update the media if needed? <yes \| no> |
| vaults | Display a list of registered Vaults. |
| vexer <*arguments*> | Run the canned Vault exercises.<br>Valid arguments:<br>• storage pool<br>• scale factor<br>• minimum file size<br>• maximum file size<br>• maximum sleep time<br>• check file? <yes \| no><br>• stop test on error? <yes \| no><br>• time to run <hh:mm:ss> |

## Vault Service

The Vault Service (**VaultSvc**) manages the Vault(s) on the network, and runs as a background service. As Vault Service runs, its behavior can be modified with the command line options listed below. You can enter a single argument, a single argument and -usage or -version, or a combination of several arguments and -usage or -version.

The command line is formed as follows:

© 2015

```
VaultSvc <option> <option> . . .
```

| Argument | Description |
|---|---|
| -instance <*number*> | Define the instance number of the Vault service to be started. |
| -service_install <*number*><br>or<br>-service_remove <*number*> | Windows only. Install is for manually installing the service. Remove is for manually removing the service. You can use only one argument at a time.<br>Valid value = service instance number |
| -usage | List all valid command line arguments for the service. |
| -version | Display the current version information. |
| -scan | Cause the VaultSvc to scan the local computer for SCSI devices and display them in the current window. The VaultSvc then terminates. |

## Configuration File Structure

The Vault configuration file provides the Vault Service with its run time operation parameters. The configuration file is read by the Vault Service at each start. The file is normally created by the Add or Remove Vault Wizard when a new Vault is added. This file is located at <install-dir>/Config/ VaultSvc<service instance number>.cfg, where <service instance number> is determined from the invocation line with the -instance command line argument (above).

Vault configuration files are formatted as follows:

```
policy_name="<Vault name>"
[
    <token>=<value>
    <token>=<value>
    . . .
]
```

### Token/Value Pairs

A token is a configuration file attribute that gives a value to determines how the service is run.

| Token | Value |
|---|---|
| act_log_enable = <*boolean*> | Enable activity logging. When enabled, all jobs, |

© 2015

| Token | Value |
|---|---|
| | retrievals, loads, ejections, startups, and shutdowns are written to the activity log.<br>Valid values = true \| false<br>Default = false |
| act_log_max_size_mb = <*number*> | The maximum size in bytes of the activity log.<br>Default = 50 (bytes) |
| act_log_pn = "<*pathname*>" | The location of the activity log.<br>Default = </usr/local/Phoenix>/Logs/VaultSvcActivity1.log |
| act_log_recycle = <*boolean*> | Write new events at the beginning of the activity log file when the maximum size is reached.<br>Valid values = true \| false<br>Default = false |
| active = <*boolean*> | Specify if the Vault should be started.<br>Valid values = true \| false<br>Default = true |
| admin_req_cmd = "<*command string*>" | If not blank, this command is executed any time offline media needs to be mounted. It may be used to execute a shell script or executable that performs an activity any time a Vault requires manual intervention.<br>The command is executed with arguments as follows:<br><command string> <host_name> <media_name> <media_storage_location><br>• host_name = the name of the client machine needing access to the media<br>• media_name = the name of the media<br>• media_storage_location = the location specified when the media was originally taken offline.<br>Default = "" (empty) |

© 2015

| Token | Value |
|---|---|
| background = <*boolean*> | For diagnostic purposes, to debug the process.<br>Valid values = true \| false<br>Default = true |
| block_size_b = <*number*> | The block size in bytes used when writing to tapes. A value of 0 (zero) indicates that a default value supplied by the host operating system is used.<br>Default = 0 |
| cache_size_mb = <*number*> | The amount of memory in megabytes allocated for the temporary storage of incoming data.<br>Default = 10 |
| cgr_id_string = "<SCSI device ID string> " | The SCSI library device or stand alone drive to be managed by the Vault. This option is only valid for data tape library Vaults and stand alone tape drive Vaults. The SCSI device ID string is composed as follows: "<Manufacturer><Product ID><Serial Number>".<br>Default="" |
| console_pn = "<*pathname*>" | The path to the file where all console activity is written.<br>Default = "/dev/console" |
| db_max_files_open = <*number*> | The number of database files that can open simultaneously. There is one database file per volume. As database files stay open, the service accesses the database files faster without extensive file opening.<br>Default = 100 |
| db_max_mem_mb = <*number*> | Limit how much virtual memory in megabytes the database uses. For best Information Repository performance, select a value that does not exceed 75% of physical memory on the computer.<br>Default = 1024 (1 GB) |
| db_opt_tod = <*mm:hh*> | The time the database is optimized daily.<br>Default = 00:00 (midnight) |

© 2015

| Token | Value |
|---|---|
| db_pn = "<*pathname*>" | The path to the folder where database files are stored. Ensure files are stored on a local hard disk.<br><br>Default = "</usr/local/Phoenix>/Database" |
| diag = <*boolean*> | Run the service in diagnostic mode. All internal activity displays on the local terminal.<br><br>• **diag** displays the minimum amount of diagnostic information.<br><br>• **diag_high** displays all diagnostic information.<br><br>Valid values = true \| false<br><br>Default = false |
| diag_high = <*boolean*> | |
| diag_pn = "<*pathname*>" | Redirect any diagnostic output to any file or device at service startup.<br><br>Default = "/dev/tty" |
| drive_id_string = "<SCSI device ID string>" | The SCSI tape drive(s) to be managed within a tape library. This option is intended to be used where the SCSI changer/library is unable to provide the correct IDs for its internal tape drives. This option may be specified multiple times for libraries with multiple drives. The first occurrence must be for the first drive with each successive occurrence for each additional drive. The SCSI device ID string is composed as follows: "<Manufacturer><Product ID><Serial Number>".<br><br>Default="" |
| email_enable = <*boolean*> | E-mail notification of certain Vault events, such as startup, shutdown, and media load requests.<br><br>Valid values = true \| false<br><br>Default = false |
| email_recipient = "<*character string*>" | The e-mail address to where e-mail notifications are sent.<br><br>Default = "" (empty) |
| email_server = "<*character string*> " | The name or IP address of the mail server. |

© 2015

| Token | Value |
|---|---|
| | Default = "" (empty) |
| error_log = "<*pathname*>" | The path to the error log file.<br><br>Default = '</usr/local/Phoenix>/Logs/VaultSvc1.log" |
| fast_index = <*boolean*> | For diagnostic use only. Enable Vault to use on-media database partitions to increase the speed that unknown media is loaded.<br><br> When "false", every load of an unknown media results in a sequential re-indexing of the entire media.<br><br>Valid values = true \| false<br><br>Default = true |
| fs_default_media_dir_pn = "<pathname>" | The default location for a hard disk Vault to store media.<br><br>Default =</usr/local/Phoenix>/Media |
| fs_max_dir_ent = <*number*> | The maximum number of files stored in a single directory contained on a unit of hard disk media. This option is valid only for hard disk Vaults.<br><br>Default = 100 |
| fs_num_virt_drives = <*number*> | The number of concurrent data connections to use at one time. This option is valid only for hard disk Vaults.<br><br>Default = 10 |
| license_string = "<*character string*>" | The 80 character ASCII text string that is contained within a license file. An empty license string causes the service to run in evaluation mode.<br><br>Default = "" (empty) |
| type="vaultsvc" | The type of configuration file.<br><br>Only valid value = "vaultsvc" |
| vault_instance = <*number*> | Define the instance number of the Vault service to start. |

© 2015

| Token | Value |
|---|---|
| | Default = 1 |
| vault_name = "<*character string*>" | The name of the Vault service that runs.<br>%HOSTNAME% and %TYPE% variables can be used instead of a hard coded name. % HOSTNAME% is replaced by the computer name; %TYPE% is replaced by the Vault's type.<br>Default = "%HOSTNAME%_%TYPE%" |
| vault_type = <*alpha*> | The type of Vault service that runs.<br>Valid values =<br>• HardDisk<br>• SingleTape<br>• TapeLibrary<br>Default = HardDisk |
| version = "<*number*>" | The version of the configuration file.<br>Valid value = "1.0" |
| working_cache_pn = "<*pathname*>" | Define the Vault's working cache directory. The working cache directory is the place where the Vault can store temporary items during its normal activities. This working cache is especially important when clipping video files.<br>Default = "</usr/local/Phoenix>/WorkingCache" |
| working_cache_size_gb = "<*number*>" | The amount of disk space the Vault's working cache may use to store temporary files. On tape Vaults, the working cache should be large enough to hold multiple large video files.<br>Default = 100GB |
| write_with_verify = <*boolean*> | For diagnostic use only. When set to true, enables the read-after-write check of most tape drives. Setting this to "false" is unadvisable as doing so can cause unreported data corruption.<br>Valid values = true \| false<br>Default = true |

© 2015

### Sample Vault Configuration File

```
policy_name = "VaultSvc1"
[
    type                      = "vaultsvc"
    version                   = "1.0"
    active                    = true
    vault_name                = "test_HardDisk1"
    vault_instance            = 1
    vault_type                = HardDisk
    db_opt_tod                = 00:00
    db_max_mem_mb             = 1024
    db_max_files_open         = 100
    db_pn                     = "/usr/local/Phoenix/Database"
    fs_default_media_dir_pn   = "/usr/local/Phoenix/Media"
    fs_num_virt_drives        = 10
    fs_max_dir_ent            = 100
    cgr_id_string             = ""
    diag                      = false
    diag_high                 = false
    diag_pn                   = "/dev/tty"
    act_log_enable            = false
    act_log_recycle           = false
    act_log_max_size_mb       = 50
    act_log_pn                = ""
    email_enable              = false
    email_recipient           = "vault_admin"
    email_server              = "email_server"
    cache_size_mb             = 10
    block_size_b              = 0
    write_with_verify         = true
    background                = true
    fast_index                = true
    console_pn                = "/dev/console"
    error_log                 = "/usr/local/Phoenix/Logs/VaultSvc.log"
    admin_req_cmd             = ""
    license_string            = ""
    working_cache_pn          = "/usr/local/Phoenix/WorkingCache"
    working_cache_size_gb     = "100"
]
```

## Windows Diagnostics

This section pertains to the Windows operating system only.

To open a diagnostics window for Vault Services, you first need to configure Windows Services to allow the Vault Service to interact with the desktop client.

© 2015

When enabling this feature, a window appears to display Vault activity. If you close this window, it stops the Vault, and Phoenix RSM does not operate without running Vaults.

To configure Vault Services to open a window for diagnostic messages, do the following:

1. Access SoleraTec Vault Service in the Windows Services window. See Start Vaults Manually for directions.
2. Stop the Vault that you want to modify. Right-click **SoleraTec Storage Vault**, and then click **Stop**. The Service Control dialog box appears briefly to display progress.
3. Right-click the **SoleraTec Storage Vault** again, and then select **Properties**. The SoleraTec Storage Vault#x Properties window (#x is the Vault ID number) appears.
4. Click the **Log On** tab.
5. Select the **Allow services to interact with desktop** checkbox.
6. Click **OK**.
7. Start the Vault. Right-click **SoleraTec Storage Vault**, and then click **Start Job**.
8. Close the Windows Services window.

# Data Services Command Line

Run DataSvcsCl to execute single, interactive migrate, replicate, and purge jobs in the Information Repository.

To run single migrate, replicate, and purge jobs, ensure that the folder where Phoenix RSM is installed is in your command path, open a command prompt, and run DataSvcsCl at the command line. Depending on what you want to do, append tokens as listed below (under Token/Value Pairs) to the execution path. For more information see Data Services Policies and Command Line Arguments.

- Access **DataSvcsCl** from your suite of application products.

## Default Data Services List Log

To see a job's run results and diagnostic information, look at the Phoenix RSM list log for any given job. Unless you change the settings and path, Phoenix RSM employs the following: %R/Logs/%P.log. You can change this value when running DataSvcsCl or in the Data Services configuration file.

## Default Data Services Error Log

To see if a job had any errors, look at the Phoenix RSM error log. Unless you change the settings and path, Phoenix RSM employs the following: %R/Logs/%P.err. This value can be changed when running DataSvcsCl or in the Data Services configuration file.

## Pathname Variables for Logs

© 2015

Pathname variables are expressions to define what information is included in your logs.

| Variable | Description |
|---|---|
| %P or %Pn | Policy Name |
| %H or %Hn | Host Name |
| %D | Date (yyyy:mm:dd) |
| %Dy | Year |
| %Dm | Month |
| %Dd | Day |
| %T | Time (hh:mm) |
| %Th | Hour |
| %Tm | Minute |
| %Ts | Second |
| %R or %Rn | Root Pathname. Valid only at the beginning of a string. |

### Command Line Options

When you run DataSvcsCl, the command line can contain a command line option or token/value pairs. As needed, append tokens as listed below (under Job Token/Value Pairs) to the execution path. The command line is formed as follows:

```
DataSvcsCl <option>
```

To retrieve usage and version information, use the appropriate option below:

- **-usage** - List all valid parameters.
- **-version** - Display the current version information.

### Job Token/Value Pairs

Use the following token/value pairs to specify policy information for the job that is going to be run.

© 2015

| Token/Value | Description |
|---|---|
| absolute_start = <*yyyy*>/<*mm*>/<*dd*>-<*hh*>:<*mm*>:<*ss*> | Used only in the policy file. The exact start time and date that the job is to run. Multiple absolute start tokens may be entered.[1] |
| active = <*boolean*> | Used only in policy file. Define whether the policy is active or inactive.<br>Valid values = true \| false<br>Default = true |
| complete = <*boolean*> | Print all summary information plus the path names of the files migrated to the file indicated by the list_pn option.<br>Valid values = true \| false<br>Default = false |
| content_filter = "<*character string*>" | A word or phrase in the file to be processed.<br>Default = "" |
| data_paths = <*number*> | The maximum number of concurrent files permitted to be sent during a job.<br>Default = 1 |
| deleted_files = <*boolean*> | Include files tagged for deletion.<br>Valid values = true \| false<br>Default = false |
| diag = <*boolean*> | Print diagnostic information to the path indicated in the list_pn option.<br>Valid values = true \| false<br>Default = false |
| dir_spec = "<*pathname*>" | Specify which directories to include. Multiple dir_spec options can be specified. The dir_spec check is made for every directory found. This includes the directories contained in the path name list that the job will traverse.<br>Default = "*" (any) |

© 2015

| Token/Value | Description |
|---|---|
| display_only = <*boolean*> | The job searches for target files without processing them. Lists the files that would have been processed.<br>Valid values = true \| false<br>Default = false |
| dst_media_name = "<*character string*>" | Specify the destination media name. If you don't specify a value in this option, The first available unit of media is used.<br>Default = "*" (any) |
| dst_media_speed = <*character string*> | Specify the destination media to be used according to media speed.<br>Valid values =<br>• S0 - S10<br>• Unspecified<br>Default = Unspecified |
| dst_media_type = <*character string*> | Specify the destination media type to be used.<br>Valid Values =<br>• Hdisk - Hard disk<br>• 8mm - Eight-millimeter tape<br>• Dds - Digital data storage<br>• Dlt - Digital linear tape<br>• Ait - Advanced intelligent tape<br>• SuperAit - Super advanced intelligent tape<br>• Vxa - Exabyte VXA tape<br>• Travan - Travan tape<br>• Lto - Linear tape open<br>• MagOptical - Read/write optical<br>• Unspecified<br>Default = Unspecified |

© 2015

| Token/Value | Description |
|---|---|
| dst_storage_pool="<*character string*>" | Specify the name of the destination storage pool to be used. Use "" for no storage pool name.<br>Default = "*" (any) |
| dst_Vault_name="<*character string*>" | Specify the destination Vault to be used.<br>Default = "*" (any) |
| dst_volume_format | Currently not supported. |
| dst_volume_name | Currently not supported. |
| dt_access=<*alpha*><*yyyy*>/<*mm*>/<*dd*>-<*hh*>:<*mm*>:<*ss*> | Process files based on the accessed date and time.<br>Valid values =<br>• AO (Absolute Old) - Selects files with a dtu (date_time_use) equal to or before the specified date. Enter the year as a 4-digit number.<br>• AN (Absolute New) - Selects files with a dtu equal to or after the specified date. Enter the year as a 4-digit number.<br>• RO (Relative Old) - Selects files with a dtu equal to or before the relative specified date.<br>• RN (Relative New) - Selects files with a dtu equal to or after the relative specified date.<br>• I (Inactive) - Do not use date.<br>Default = I |
| dt_stored=<*alpha*><*yyyy*>/<*mm*>/<*dd*>-<*hh*>:<*mm*>:<*ss*> | Process files based on the date and time stored on the Vault.<br>Valid values =<br>• AO (Absolute Old) - Selects files with a dtu (date_time_use) equal to or before the specified date. Enter the year as a 4-digit number.<br>• AN (Absolute New) - Selects files with a dtu equal to or after the specified date. Enter the year as a 4-digit number. |

© 2015

| Token/Value | Description |
|---|---|
| | • RO (Relative Old) - Selects files with a dtu equal to or before the relative specified date.<br>• RN (Relative New) - Selects files with a dtu equal to or after the relative specified date.<br>• I (Inactive) - Do not use date.<br>Default = I |
| error_log = "<*pathname*>" | Specify the path for the error log file. If you specify "/dev/tty", error messages display on the default output device. Supports token substitution.<br>Default path for the configuration file = "%R/Logs/%P.err"<br>Default path for the command line = "/dev/tty" |
| exclude_dir_spec = "<*pathname*>" | Omit directories. Accept multiple instances.<br>Default = "" (no directories excluded) |
| exclude_file_spec = "<*pathname*>" | Omit files. Accept multiple instances.<br>Default = "" (no files excluded) |
| file_spec = "<*pattern*>" | Set the criteria for files that are to be processed. This token/value pair can be specified multiple times to include multiple file filters.<br>Default = "*" (any) |
| hostname = "<*host name*>" | Select the files that are to be processed based on the original host name for the file.<br>Default = "" |
| include_offline = <*boolean*> | Process files from offline media.<br>Valid values = true \| false<br>Default = false |
| job_type = <*alpha*> | Specify the job type.<br>Valid values =<br>• replicate<br>• migrate |

© 2015

| Token/Value | Description |
|---|---|
| | • purge<br>Default = migrate |
| keep = <*boolean*> | Keep a copy of the source files after they have been processed.<br>Valid values = true \| false<br> You would use "false" to create a move policy; use "true" to create a replicate policy.<br>Default = false |
| list_pn = "<*pathname*>" | Specify the file where all report information is written. Supports token substitution.<br>Default path for the policy file = "%R/Logs/%P.log"<br>Default path for the command line = "/dev/tty" |
| max_file_size = <*number*> | Specify the maximum size in bytes of a source file. The min_file_size and max_file_size options are mutually exclusive.<br>Default = 18446744073709551615 |
| min_file_size = <*number*> | Specify the minimum size in bytes of a source file. The max_file_size and min_file_size options are mutually exclusive.<br>Default = 0 (none) |
| out_of_band = <*boolean*> | Enable the application to constantly monitor its processes and select the network transmission protocol that best suits the files being processed.<br>Valid values = true \| false<br>Default = true |
| post_proc_cmd = "<*command*>" | Specify a command that runs immediately after the job is finished. Supports token substitution.<br>Default = "" |
| pre_proc_cmd = "<*command*>" | Specify a pre-process command that runs immediately before a job starts. Supports token substitution. |

© 2015

| Token/Value | Description |
|---|---|
| | Default = "" |
| remove_only = <*boolean*> | Purge the targeted file from the source Vault instead of migrating or replicating it.<br>Valid values = true \| false<br>Default = false |
| repeat_interval = <*hh:ss:mm*> | Used only in the policy file. The amount of time that elapses before a job is repeated.[1]<br>Default = 24:00:00 |
| src_high_water_mark = <*number*> | Specify the maximum percent (%) of media that will be used. If the % used is greater than the entered value, the file is processed.<br>Valid values = 1 - 100<br>Default = 0 |
| src_low_water_mark = <*number*> | Specify the minimum percent (%) of media used after the high watermark has been reached. If the % of media used is greater than this value and the high watermark has been reached, the file is processed.<br>Valid values = 1 - 100<br>Default = 0 |
| src_media_name = "<*character string*>" | Specify the source media name.<br>Default = "*" (any) |
| src_media_speed = <*character string*> | Specify the source media speed.<br>Valid values =<br>• S0 - S10<br>• Unspecified<br>Default = Unspecified |
| src_media_type = <*character string*> | Specify the source media type from the file.<br>• Hdisk - Hard disk.<br>• 8mm - Eight-millimeter tape. |

© 2015

| Token/Value | Description |
|---|---|
| | • Dds - Digital data storage.<br>• Dlt - Digital linear tape.<br>• Ait - Advanced intelligent tape.<br>• SuperAit - Super advanced intelligent tape.<br>• Lto - Linear tape open.<br>• Vxa - Exabyte Vxa tape.<br>• Travan - Travan tape.<br>• MagOptical - Read/write optical.<br>• NullDevice<br>• Unspecified<br>Default = Unspecified |
| src_storage_pool = "<*character string*>" | Specify the source storage pool.<br>Default = "*" (any) |
| src_Vault_name = "<*character string*>" | Specify the source Vault.<br>Default = "*" (any) |
| src_volume_format | Currently not supported. |
| src_volume_name | Currently not supported. |
| start_days = <*mtwtfss*> | Used only in the policy file. Specify the days the job is to run. Use **-** to indicate days that job does not run.<br>For example, if the job is to run on Thursday, type ---t---.[1]<br>Default = mtwtfss |
| start_time = <*hh:mm:ss*> | Used only in the policy file. Specify the time the job should start for each defined start day in start_days.[1]<br>Default = 0:0:0 (midnight) |
| stop_time = R<*yyyy*>/<*mm*>/<*dd*>-<*hh*>:<*mm*>:<*ss*> | Used only in the policy file. Specify the date and time the job is to stop. The date and time entered is relative to the start of the job. |

© 2015

| Token/Value | Description |
|---|---|
| | Default = 0/0/0-0:0:0 (no stop time) |
| summary = <*boolean*> | Print the start and stop times and final statistics of the job to the file indicated by the list_pn option (above).<br>Valid values = true \| false<br>Default = true |
| throttle = <*number*> | The throttle controls the amount of bandwidth used by jobs (and the speed that files are sent to Vaults). Throttle values are relative to Information Repository capacity and range from 1% to 100%. A lower setting reduces the amount of available bandwidth.<br>Valid values = 1 - 100<br>Default = 100 |
| type = "<*alpha*>" | The policy type of the policy file. Only "ds" is valid for Data Service policies. |
| vcs = <alpha><*number*> | Specify the number of files (F) or number of bytes (S) to store per single Vault connection.<br>Valid values =<br>• F - files<br>• S - bytes<br>• 1 - ∞<br>Default = F500 |
| version = "<*number*>" | The version number of the currently installed command line application. Only the current version number is valid. This number changes with new releases. |
| volume_use | Currently not supported. |

[1]**Note:** Timing tokens are mutually exclusive. Only one timing token may be set. Set either absolute_start, or repeat_interval, or start_days and start_time.

© 2015

## Data Services Service

The Data Services Service (**DataSvcsSvc**) runs automated migrate, replicate, and purge jobs in the Information Repository using Data Service Policies. For the Data Services Service to execute, Phoenix RSM must have a policy that specifies everything needed to process targeted files. A targeted file is any file that meets all the criteria defined in the policy.

As DataSvcsSvc runs, its behavior can be modified with the command line options listed below. You can enter a single argument, a single argument and -usage or -version, or a combination of several arguments and -usage or -version.

The command line is formed as follows:

```
DataSvcsSvc <argument> <argument> . . .
```

| Argument | Description |
|---|---|
| -config "<*pathname*>" | Specify the file that contains all job criteria.<br>Default = "<install-dir>/Phoenix/Config/DataSvcsSvc.cfg" |
| -diag<br>-nodiag | Run the service in diagnostic mode. All internal activity displays on the local terminal.<br>Default = -nodiag |
| -diag_pn "<*pathname*>" | The path where all diagnostic information is written.<br>The default path is "/dev/tty" |
| -error_log "<*pathname*>" | The path for the error log file.<br>The default path is "<install-dir>/Phoenix/Logs/DataSvcsSvc.log" |
| -foreground<br>-background | For diagnostic purposes to debug the process.<br>This option is for UNIX only.<br>Default = -background |
| -list_pn "<*pathname*>" | Specify a path for verbose output. (See "-verbose" below.)<br>Default = "/dev/tty" |
| -service_install <*number*><br>-service_remove <*number*> | Windows only.<br>• Install is for manually installing the service.<br>• Remove is for manually removing the service. |

© 2015

| Argument | Description |
|---|---|
| | Default = the service instance number. |
| -update_int <*seconds*> | Specify the configuration update interval. If the -config file is modified during the job session, the Information Repository re-reads it. To disable this option, set the interval to 0.<br><br>Default = 60 |
| -usage | List all valid parameters. |
| -verbose<br><br>-noverbose | Control whether progress information is printed to the path indicated in the -list_pn command.<br><br>• **Verbose** - causes progress information to be printed.<br><br>• **Noverbose** - causes progress information not to be written.<br><br>Default = -noverbose |
| -version | Display the current version information. |

## Live Viewer Command Line

Start the Live Viewer from a command line and set options on how to view it. The command line is formed as follows:

```
LiveViewer <option> <option> . . .
```

© 2015

| Option | Description |
|---|---|
| -patrol "<patrol name>" | Starts the Live Viewer with the entered patrol.<br>Quotes are required if the name has any spaces in it.<br>The patrol names are not case sensitive on the command line.<br>If -patrol and -layout are both specified, then the first encountered option is used and the other is ignored. |
| -layout "<layout name>" | Starts the Live Viewer with the entered layout.<br>Quotes are required if the name has any spaces in it.<br>The layout names are not case sensitive on the command line.<br>If -patrol and -layout are both specified, then the first encountered option is used and the other is ignored. |
| -delay <sec> | Delays the start of the Live Viewer by the number of seconds entered. The default is 0 (no delay). |
| -fullscreen <screen #> | Maximize the Live Viewer, but also removes the Title bar and the Windows Start bar at the bottom of your monitor. This option overrides -maximize. |
| -maximize <screen number> | Displays the entire Live Viewer to maximum size on the screen. The screen number is the screen to display the maximized Live Viewer on if there are multiple screens. |

For more information see Live Viewer.

# Job Scheduling

Job scheduling windows are evident when creating policies; they determine when those policies should run as jobs. The jobs can be scheduled to run on various dates and times.

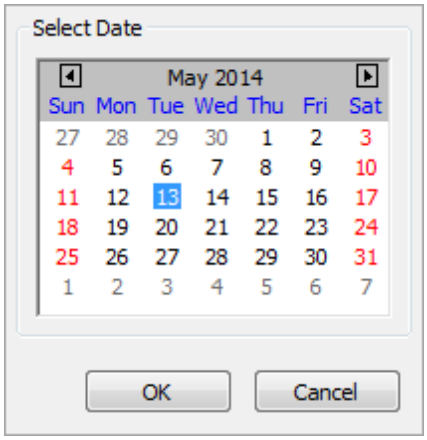
If you want to save captured video to a Vault, a Camera Policy is necessary to setup. It is recommended to create policies as soon as Phoenix RSM is configured and installed. You do not have to allow a certain amount of time to pass in order to implement policies to optimize storage capacity. To maximize Phoenix RSM's data asset management capabilities, be sure to implement a Data Service Policy to migrate, replicate, or purge data on network Vaults, or to near-line or offline storage devices.

When creating these policies, on the **Scheduling** tab, use the following job scheduling windows to support the policy implementation process.

© 2015

## Date window

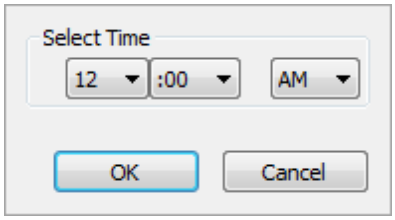
Use to set a date for when your job is to run.




1. Using the arrow buttons by the month and year at the top, set your month and year preference.
2. Click a particular day from the calendar.
3. Click **OK**. (Click **Cancel**, to close the dialog box without saving new or changed parameters.)

## Time window

Use to set a time for when your job is to run.

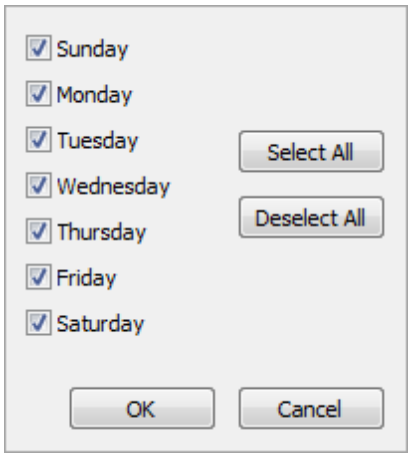



1. From the drop-down lists, select the hour and minutes for your time preference, and then select either AM or PM.
2. Click **OK**. (Click **Cancel**, to close the dialog box without saving new or changed parameters.)

## Days window

Use to define on which days of the week a job is to run.

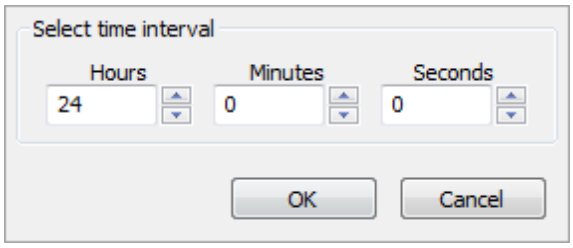
© 2015




1. Select the day(s) you want the job to run.
2. Click **OK** to save the values to the policy. The selected days appear in the **On what days of the week** text box. (Click **Cancel**, to close the dialog box without saving new or changed parameters.)

## Duration window

Use to set a maximum time that a job should be allowed to run.



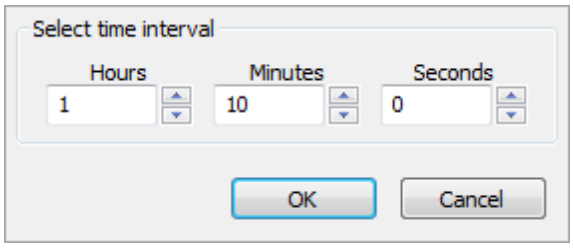

1. Set the duration using the Hour, Minutes, and Seconds boxes. The job terminates after the duration time is met.
2. Click **OK**. The **Should the job be stopped before it is completed** text box displays the duration of the job before it terminates. (Click **Cancel**, to close the dialog box without saving new or changed parameters.)

## Time Interval window

Use to set the time interval to run your jobs at. The job runs at the interval entered until it is changed. To stop a job that is using the repeat setting, edit or delete the policy.

For example, to run a job every three hours, enter 3:00:00; once a day, enter 24:00:00; every two days, enter 48:00:00. If you enter 3:30:30, the job repeats every three hours, thirty minutes, and thirty seconds from the time the policy is saved.

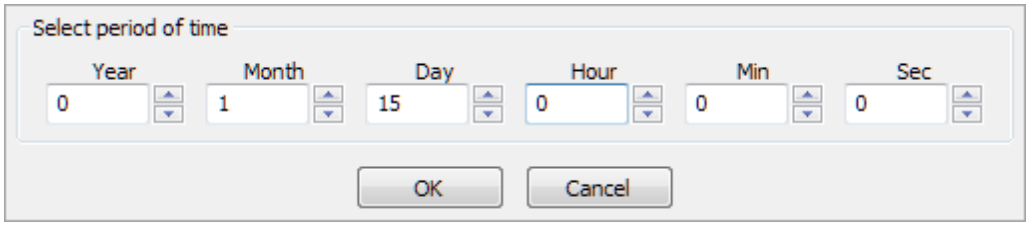
© 2015




1. Set the time interval for the job to run using the Hours, Minutes, and Seconds boxes. The clock for the interval begins as soon as you save the policy.
2. Click **OK**. (Click **Cancel**, to close the dialog box without saving new or changed parameters.)

### Period of Time window

Use to search for files that have been modified within a defined period of time.




1. Enter a period of time in terms of years, months, days, hours, minutes, or seconds. Enter any combination or up to a maximum period of 10 Years, 100 Months, 1000 Days, 100000 Hours, 1000000 Minutes, and 1000000 Seconds.
2. Click **OK**, and the text box where you started from displays the value entered. (Click **Cancel**, to close the dialog box without saving new or changed parameters.)

# Troubleshooting

The following are frequently asked questions and common issues that you may come across during the course of using SoleraTec's Phoenix RSM. The categories listed below mention the issues and then discuss the possible causes to lead you towards a resolution. See the appropriate heading for details.

### Vault Issues

| Issue | Possible Causes |
|---|---|
| **Cannot see my Vaults?** | • Check that the Surveillance Feature is enabled and the NAS is running.<br>• Check that NAS has a static and valid IP address. |

| Issue | Possible Causes |
|---|---|
| | • Check that multicast routing is enabled if using a smart switch.<br>• Is there a security software blocking multicast?<br>• Enable our multicast address - 224.0.23.160, enable traffic, and check your firewall.<br>• Check that local firewall is not blocking any applications.<br>• If the desktop computer has multiple network devices, try disabling them and reboot.<br>• Try using a static IP address on the desktop computer.<br>• Check if application is being blocked by Windows UAC.<br>• If running Vmware, disable Vmware network connections.<br>• Restart the NAS. |
| **My Vault keeps stopping?** | • Restart the NAS.<br>• Check that the Vault license is current after Vault is seen. |
| **My Vaults are filling up.** | • Watermarks are not set up properly.<br>• In Data Services Policies, on the **Criteria** tab, there are options to order the type of media (like data tape, or optical) or purge dispensable data. |
| **My Vault does not see my data tape drive or data tape library.** | • Check the data tape drive and data tape library configurations for your computer; the Add and Remove Vault wizard will not be able to communicate with the device.<br>• Check for connection using the “device manager” for your operating system.<br>• Disable the SCSI connection. Disabling does not affect the software’s use of the device. |

## Camera Issues

| Issue | Possible Causes |
|---|---|
| **My camera connection fails.** | • “Live View” must be checked in Camera Configurations to allow access by Live Viewer.<br>• Check that the camera is powered and configured |

© 2015

| Issue | Possible Causes |
|---|---|
| **I cannot live view the camera.**<br><br>**I cannot test view the camera.** | according to manufacturer's recommendations.<br>• Check that the camera has a valid static IP address configured.<br>• Check that the camera is not blocked by a local or remote firewall.<br>• Validate that the camera IP address, manufacturer, model, user name, and password settings are correct in the Camera Configurations.<br>• Validate the RTSP URL using VLC Media Player.<br>1. Once installed, go to **Start** > **All Programs** > **VideoLAN** > **VLC media player**.<br>2. In the VLC media player Media menu, select **Open Network Stream**.<br>3. Type the RTSP URL and click **Play**. Verify a connection. If there is no connection here, check the camera.<br>• Ping the IP address to verify connectivity.<br>1. Go to **Start** > **All Programs** > **Run**.<br>2. In the Run window type **cmd**.<br>3. In the command prompt window, type **ping <camera IP address>**, and wait for a response. If no connection, the camera may be off.<br>• If remotely connected to a computer, video may not play correctly. |
| **All of my camera configurations and recording policies are missing.** | • Check that the NAS is running correctly.<br>• Has the NAS been "factory reset" or storage re-initialized? Must recreate configurations.<br>• Were they manually deleted? |
| **My camera is not recording.** | • Camera does not exist in Camera Configurations.<br>• Camera is not enabled in Camera Configurations.<br>• Recording policy is not enabled in Camera Policies.<br>• Recording computer selection is not valid in Camera Configurations. |

© 2015

| Issue | Possible Causes |
|---|---|
| | • No license.<br>• License is expired.<br>• See resolutions for “Connection fails” above.<br>• The NAS has run out of storage. |
| **My cameras do not show up in a camera search.** | • Camera is not powered on.<br>• Camera is not connected to network.<br>• Camera is not configured per installation instructions.<br>• Auto discovery is not enabled on camera.<br>• Camera does not support auto discovery. Must enter IP address manually. |
| **My camera video is poor quality.** | • Camera is low quality.<br>• Camera is configured to high compression.<br>• Camera is configured to small frame size.<br>• Lighting is insufficient.<br>• Camera is malfunctioning. |
| **How do I install camera drivers?** | • Camera drivers are not required. |
| **I removed and replaced my drives, now my cameras are not recording and my video is not playable.** | • Vault has marked the drives as being offline. You must reload all media.<br>1. Open Vault Admin.<br>2. Expand Media tree item.<br>3. Right-click on each media and select “Reload Media”. |
| **My camera is not viewable in Live Viewer when using “Remote Desktop” or VNC.** | • Video is not always playable through remote connections because of hardware considerations. Try another tool such as “Log Me In”, or “Team Viewer”. |
| **How do I know if my camera is recording?** | • Wait 10 minutes and do a video search using “Surveillance Video Manager”.<br>• Check that there are no yellow warning triangles in Camera Policies or Camera Configurations. |

© 2015

| Issue | Possible Causes |
|---|---|
| | • Check the LCD panel on the NAS for an error condition.<br>• Check the NAS Web UI for an error condition.<br>• Check the log files (Advanced user only). |
| **Asterisks in the camera list.** | • Camera is not active and is ready to be configured. |
| **My applications and camera stop functioning after a change.** | • Check network and DHCP settings. Applications may not work if there have been any network or DHCP changes.<br>• Each Vault should be assigned a static IP address.<br>• Check IP network camera connectivity and active status if Camera Policies stop working. |
| **How does my software handle camera connections?** | • Video is streamed to the recording server when the camera is scheduled to record. Video is also streamed directly from a camera to any Live Viewer session which is watching that camera. |
| **Not seeing the date and time from the camera manufacturer.** | • Log into the camera's management utility to 'enable' the date and time stamp overlay. Phoenix RSM relies on the network IP camera to superimpose the date and time onto the recorded video. |
| **Thumbnails do not generate with my camera.** | • Disable the audio setting (if it has audio). Some older cameras do not correctly stream video and audio together. |
| **Forgot camera password on the wizard.** | • Check with your camera's user manual for password setting or for resetting the camera. |
| **Video freezes in low light conditions.** | • Set the Live Viewer video stream delay value to a larger value to prevent the image from freezing, especially on slow frame rate high definitions cameras.<br>1. Open Live Viewer<br>2. Select camera view frame.<br>3. From the **Tools** menu, select **User Preferences**.<br>4. From the **Video Stream Delay** drop-down list, select a larger value, such as **700ms** or greater.<br>5. Click **Save**. |

© 2015

## Video Issues

| Issue | Possible Causes |
|---|---|
| **I am running out of NAS storage for video.** | • Default Data Service Policy purge named "RemoveOldVideo" has been disabled or deleted. Either enable it or create a new purge policy.<br>• Other NAS applications are using up storage. Install another NAS to store more surveillance video. |
| **My search results thumbnails look like a "fake picture".** | • Thumbnails are disabled in recording policy.<br>• Video from camera is not in a supported format. |
| **When I export video, why can't I play it?** | • Video format is not supported by your video player. Try VLC.<br>• Video is corrupted from camera. |
| **Cannot see thumbnail or low resolution companion/proxy video.** | • Ensure the **Generate low resolution proxy** and **Generate preview image** options are selected In Camera Policies, on the **Processing** tab.<br>• Ensure the **Generate low resolution proxy** and **Generate preview image** options are selected from the Camera Policies window > **Tools** menu > **User Preferences**. |
| **My export procedure does not complete to 100%.** | • Ensure you have proper versions of VLC or QuickTime on your computer. When exporting a video segment (or "Clip") that spans a number of video files from storage, one of the final steps in the export procedure is "stitching" the segments together. The Export process gets close to 100%, but then fails. |

## Search Issues

| Issue | Possible Causes |
|---|---|
| **My search results do not populate with video?** | • Ensure a correct camera is selected in the Search Criteria pane.<br>• Try searching without selecting a camera. |

© 2015

| Issue | Possible Causes |
|---|---|
| | • Other search options are selected which do not match any video or cameras. Clear all of these selections and search again.<br>• Try closing the application, restarting, and then press Search.<br>• Ensure the camera has a recording policy configured.<br>• Ensure the created camera policies are saved. Go to the Camera Policies application to view the policies.<br>• Check the parameters associated with the camera policy.<br>• Is the camera configured to record video for the times you are searching?<br>• The NAS is not running.<br>• The NAS is not properly licensed.<br>• A firewall is blocking access to the NAS.<br>• Times on NAS, cameras, and desktop computers are not synchronized. |
| **Cannot find or add metadata.** | • Metadata search options appear in Camera Policies and SVM only if there is a MetadataExtensions.cfg file in <install directory>\Config<br>• Ensure that the MetadataExtensions.cfg file is on every computer where it would be modified.<br>• Look in documentation for instructions on creating the needed files. |
| **How do I tell if export extensions are running?** | • The extension is a piece of user code that is invoked when exporting files. It could be a shell script, Perl script, compiled program, built in utility or something similar.<br>1. Develop and debug your script in a standalone environment. Run it from a terminal or command prompt before integrating it with SVM.<br>2. The script should send logging to the screen or a file. At the least, it should log any input parameters to a file so you can see if it is running correctly or at all.<br>3. Try running a simple alternative program from SVM to see if the framework is set up correctly. It could do something as simple as echoing text to the screen, or touching a file. |

© 2015

| Issue | Possible Causes |
|---|---|
| | 4. Many times problems are path or permission related, especially if the extension script is developed on a different machine than the final target. Make sure your script is in the Phoenix RSM Bin directory and has execute permission. Ensure Perl or Python are installed (if needed), and the path to find them is set up correctly. |

## Media Issues

| Issue | Possible Causes |
|---|---|
| **With SAN or NAS, my media goes offline.** | • Your SAN or NAS may have become unavailable. When this happens, the Phoenix RSM media resident on the SAN or NAS are marked as offline. They need to be brought back online using Vault Admin. Right-click on each offline media and select **Reload media**. |
| **With unloaded media, I cannot get back to it or find it.** | • Check the default location for the media; it may have changed.<br>• Check for correct paths to media. |
| **My data tape drive is slow.** | • Check number of files in throughput.<br>• Check the size of files in throughput.<br>• Check if there is congestion on the network.<br>• Operating system determines the throughput speed. |

## Network Issues

| Issue | Possible Causes |
|---|---|
| **Nothing works after I change my network address.** | • You must reboot your desktop computer if it changes networks or addresses. |
| **Nothing works after my computer wakes from sleep mode.** | • Disable sleep mode on your computer. |

© 2015

| Issue | Possible Causes |
|---|---|
| **Numbers rather than policies are in Host IDs.** | • Check to see if the Locator Service or Services have stopped.<br>• Reboot your computer.<br>• Manually restart the service. |
| **When loading and installing a new version to Apple, it does not update correctly.** | • Be sure that files have not been moved since the original installation. If files are moved, the Apple Installer updates those moved files where they currently exist instead of the Phoenix RSM installation folder in Applications.<br>• Try uninstalling the software and installing new copy. |
| **Problems with network connectivity and my Apple laptop.** | • Ensure connection to an active network. If laptop is not connected to a LAN, the applications may not function properly. |
| **Live Viewer causes my CPU to respond slowly, or I get a wait screen.** | • Check the current system requirements.<br>• Be aware of CPU speed, and disk read/write capacity.<br>• Check network congestion and connectivity. |
| **When searching, it cannot find files that other people see on the same network.** | • Check permissions on data. |
| **Can't run on Windows 2000 or older.** | • Check the current system requirements. |
| **My Data Service Policies do not run to completion (files are not moved).** | • Ensure storage resources are active.<br>• Ensure there is enough storage space available. |
| **Cannot find software when making advanced changes to the registry.** | • Check registry for the company name, then the product name. (For example: CompanyXYZ, ProductXYZ) |

## Error Messages

© 2015

| Issue | Possible Causes |
|---|---|
| **With recorded video, the error "Unable to retrieve resource" displays.** | • Verify the Vault is online; check if powered down, check network connectivity, and check connectivity of the Vaults.<br>• Keep in mind that original video data from a single source may be stored on various Vaults and if those Vaults are not online then the video may generate this error. |
| **As my job runs, the errors "Unable to allocate resources" or "Cannot find Vaults" display.** | • Check network connectivity.<br>• Check space availability on media.<br>• Ensure the Locator Service has not stopped.<br>• See troubleshooting entry "Cannot see my Vaults". |
| **"Libraries not available" warning displays when starting applications in Linux** | • Libraries that are required for correct Phoenix RSM operation are not installed on your machine. Install the requested libraries shown in the message. |
| **My Vault is shown with a "RPC Error" message in Vault Admin.** | • Vault or NAS is not running correctly. Reboot the NAS.<br>• Your desktop network configurations are not correct.<br>• Your NAS network configurations are not correct.<br>• NAS is on a different subnet which is not accessible. |
| **I receive an "Rvt" error when starting any GUI application.** | • Local Locator Service is not running. Reboot machine.<br>• Firewall settings are blocking correct network operation.<br>• Windows UAC is blocking correct application operation.<br>• Application was not started from "Start" menu on Windows.<br>• Client software was installed as "For my use only". Re-install for all users. |
| **Where are the system log files for the NAS?** | • Look in the Phoenix RSM share.<br>• Log files are best read with WordPad (Windows) or TextEdit (Apple). |
| **The Recording Computer field shows "Not found".** | • Check that the NAS is running correctly.<br>• Has the NAS been "factory reset"? Must reselect recording computer. |

© 2015

### Licensing Issues

| Issue | Possible Causes |
|---|---|
| **My Product Key or license is not valid.** | • May have been activated previously on a different NAS.<br>• Is a demo product key and is now expired.<br>• Cannot move product keys between NAS units. |

### Log files

Log files are system output files that can help diagnose or track warnings, issues, and problems with the applications. The following provide insight as to what a log file might include. Each log file should be analyzed and treated individually.

**LocSvc.log** - Reports networking/NIC issues.

**DataSvcsSvc.log** - Reports problems mainly related to job scheduling of Data Service policies. For example, warnings at startup, no active Vaults, a Vault is not yet registered, or no found jobs to run. When a Vault does start, Data Services Service picks up its jobs to run.

**Vault.log** - Contains errors, warnings, or informational messages from the VaultSvc. Normally, for every start message you should see a stop message. If there is another start message immediately following the first start message, then the VaultSvc was not properly stopped in its previous run. “CYA” messages are informational messages for Phoenix RSM. There is no loss of data, only a warning that the database had to be rebuilt/re-indexed.

**Purge When 80Pct Full.log** - Log entries report a summary of the Data Service Job (Purge When 80Pct Full) running. Every Data Service policy that runs produces this file with job information. If there are any errors or warnings, it also creates an “.err” version of the same file.

**<policy>.log** - A Camera Policies log file, summarizing information which only shows video being sent to the Vault.

**<policy>.err** - A Camera Policies log file, showing any problems with sending video to a Vault.

**<policy>_capture.err** - A Camera Policies log file, displaying any problems capturing video from a camera.

If the .err files contain repeating sequences of errors at regular intervals, that would indicate an on-going error. Otherwise, the errors most likely corrected themselves

# Manage Services

At times it may be necessary to manually start or stop SoleraTec services. The following sections outline the necessary procedures to perform these tasks.

© 2015

Depending on the components installed on your machine (i.e. **server** or **client**), not all of these services may be available.

| Service Name | Service Description |
|---|---|
| LocSvc | SoleraTec Locator Service |
| VaultSvc1 | SoleraTec Vault Service |
| VaultSvc2 | |
| VaultSvc3 | |
| VaultSvc4 | |
| TgtProcSvc | SoleraTec Target and Process Service |
| DataSvcsSvc | SoleraTec Data Services Service |

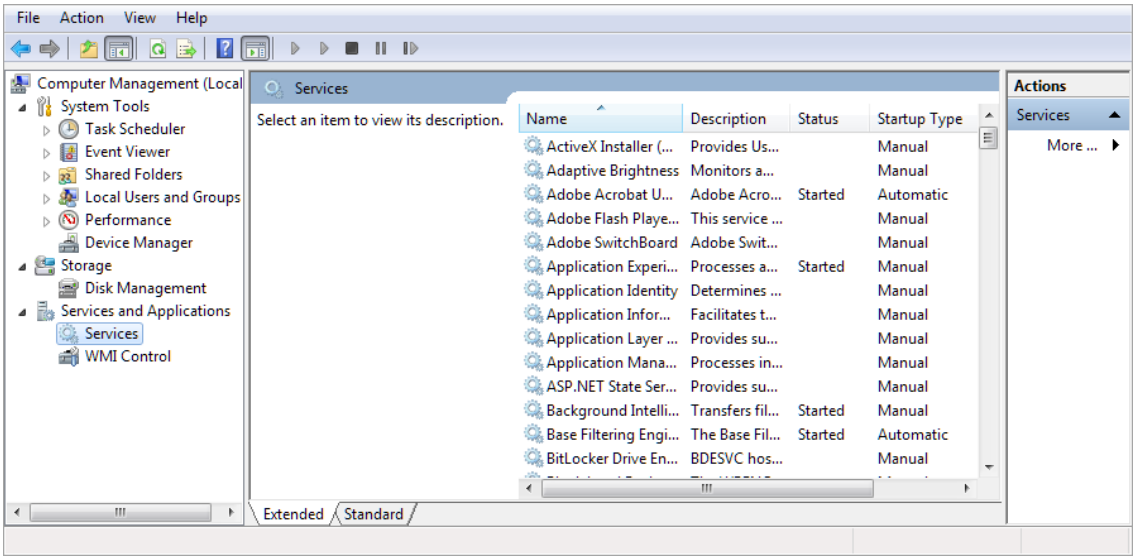
## Windows

Use **Windows Services** to **Start** and **Stop** services.

You may need Windows administrator rights for performing certain tasks (administrators have complete and unrestricted access to a computer or domain). General information is provided by Microsoft.

1. Hold the **Windows Logo** key and the **R** key to open the **Run** dialog box.
2. Enter **services.msc** and click **OK**. The **Services** window will open.
3. Scroll down to find the desired Service. For example, SoleraTec Locator Service.

© 2015




4. Right-click the desired Service, and then select **Start** or **Stop**. If the actions are disabled, check your Windows administrator rights.

Services will automatically restart when the machine is restarted.

## Mac

1. Click **Go**, then choose **Utilities**.
2. Double-click **Terminal**.
3. Enter a command:
   - To **Start** a service: `$ sudo /bin/launchctl load /Library/LaunchDaemons/com.SoleraTec.<Service name>.plist`
   - To **Stop** a service: `$ sudo /bin/launchctl unload /Library/LaunchDaemons/com.SoleraTec.<Service name>.plist`

**<Service name>** is replaced with one of the following:

| Service Name | Service Description |
|---|---|
| LocSvc | SoleraTec Locator Service |

© 2015

| | |
|---|---|
| VaultSvc1 | SoleraTec Vault Service |
| VaultSvc2 | |
| VaultSvc3 | |
| VaultSvc4 | |
| TgtProcSvc | SoleraTec Target and Process Service |
| DataSvcsSvc | SoleraTec Data Services Service |

Services will automatically restart when the machine is restarted.

# Glossary

**A**

**ACL** - ACL stands for access control list. It is a table that tells a computer operating system the access rights that each user has to a system object, such as a file directory or an individual file. Each object has a security attribute that identifies its access control list. The list has an entry for each system user with access privileges. The most common privileges include the ability to read files, to write files, and to execute the files.

**Administrator** - Administrators have complete and unrestricted access to a computer or domain.

**Analog camera** - A surveillance camera which uses older technology video cable to transfer images to a recording device, such as a VCR. It is similar to the yellow RCA/BNC cable that older television sets use to connect to a VCR.

**Analytics** - A technology used to analyze video for specific data, behavior, objects or attitude. It can be used to automate alarms and make searching through video easier.

**Automatic fail-over** - If there is more than one Vault available, clients can divide their use of the available Vaults. Clients fail-over from the current Vault in use to another Vault, should the current Vault fail.

**B**

**C**

**Camera Policies** - A policy is a set of rules which define how to record video from cameras.

**Camera Pool** - A camera pool is a user defined virtual grouping of cameras used to search video from specified cameras. For example, suppose you have a camera pool called "Doors". It is comprised of all the cameras that watch over the doors of your business. When you need to see who's come or gone, select the "Doors" camera pool as a search criteria, and only video captured from this camera pool are included. There is no limit to the number of camera pools your Phoenix RSM solution may have.

© 2015

**Channel** - The name traditionally used to describe the connection between a camera and the recorder.

**CIF** - CIF refers to the size of the video in pixels. CIF is a video image 352x288. Other common sizes include QCIF (176x144), 4CIF (704x480), and 16CIF (1408x1152).

**Client** - Clients provide interfaces for system administrators and end users. With Phoenix RSM's balanced, extended client/server architecture, clients often play roles normally supported by servers. This enables increased Information Repository flexibility, security, robustness and capacity.

**Clip Name** - Most video editing systems and digital cameras have a machine-assigned file name (such as 123abc_ffx2) for a piece of video. "Clip Name" is a metadata value of a human-assigned name (such as jon_talking) for that video clip. Clip Name is also used by the video editing systems to identify a video. Both the machine-assigned filename and the human-assigned clip name are searchable in Phoenix RSM and therefore are separate search criteria.

**Collapsing Data** - When data is removed from the primary hard disk storage tier and replaced with a pointer file. A copy of the file exists in the Information Repository and a pointer to the file exists in the computer's file system. Data that is collapsed appears to the networked computer's file system as if it resides locally.

**Communications Timeout** - If the product is unable to connect with a computer on the network or communications are interrupted during a job, it waits a predefined period of time before completely dropping the connection. This period of time is called the "communications timeout."

**Component** - A component is a single application or utility that could interact with or have dependencies on other applications. Phoenix RSM software consists of several separate components that work together to protect your files.

**CRC** - Cyclic redundancy check is used to ensure data integrity by detecting accidental alterations of data during transmission or storage. A unique numeric value is assigned to captured or ingested files, and then an algorithm calculates this value based on data stream, file size, and other characteristics. The CRC value is compared on client and server, and validated.

**D**

**Data Service Policies** - These policies are sets of rules which define how the videos or files are duplicated, moved, or deleted across multiple storage devices.

**Data Services Service** - Data Services Service enforces or implements the Data Service Policies.

**Default** - A default value or setting used by a device or program when no other value or setting has been specified.

**DHCP** - A network configuration protocol used to assign addresses to computers on a network.

**Digital camera** - A surveillance camera which uses newer network cable to transfer images to a recording computer, such as a NVR. These cameras connect to your network like your computer.

**Digital fingerprinting** - A checksum (or digital fingerprint) that uniquely identifies video with a "fingerprint". It is a numerical value calculated from the SHA256 hash algorithm.

**DVR** - A device which records video from an analog source, converts it to a digital format, and then stores it on a disk or some other similar storage medium.

© 2015

**Dynamic resource allocation** - The process used by Phoenix RSM to find and use storage resources that may be available across multiple storage devices.

**E**

**Encoder** - A device which takes the video signal created by an analog camera and converts it to a digital format as created by newer digital cameras. It is most often seen when using older cameras in newer digital systems.

**F**

**Forensics** - The process of reviewing recorded surveillance video to determine what happened in the past. Phoenix RSM is a forensic video system.

**Frames per second (FPS)** - Frames per second, is an expression of frame rate. Surveillance cameras record anywhere from less than 1 FPS to greater than 30 FPS. For the best chance of conviction based on video evidence in a court of law, chain of custody procedures require 30 FPS.The higher the frame rate, the smoother the video looks.

**G**

**H**

**H264** - A term used to describe the format of digital video. H264 is commonly used by digital surveillance cameras.

**Header** - In data storage, a header is an area on media where the parameters assigned during preparation of the media are stored. The information contained in the header includes access control lists (ACL), storage pool information, media size, type, etc.

**Histogram** - Statistically, a histogram visually shows the distribution of data.

**Host** - The computer where files originate or where the policy resides.

**I**

**Information Lifecycle Management (ILM)** - The policies, processes, practices, and tools used to align the business value of information with the most appropriate and cost-effective IT infrastructure from the time information is conceived through its final disposition. When ILM is video aware, it is called Video Lifecycle Management (VLM).

**Information Repository** - The Information Repository is where data is stored. Since a Vault is a storage device used to store files, the Information Repository is made up of all the storage devices, clients and Vaults on your network.

**Ingesting** - The process of using Phoenix RSM clients to archive or move data, including metadata, from a networked computer into the Information Repository. Capturing video from RTSP enabled IP cameras is a type of ingesting.

**J**

**K**

**L**

© 2015

**Label** - A label (or media label) is a name assigned to a unit of media. Assigned manually to media, unless a barcode system is available, the labels are used for media identification. If a barcode system is in use, the label name is superseded by the barcode on the media. When media is loaded into a drive, the Information Repository's first task is to read the label to identify and ensure that the proper media unit is being used.

**lic** - File extension for a license file. To be seen by the Information Repository, the license file(s) must be in the <install-dir>/Config folder.

**Live Viewer** - The application that is used to watch what is being seen by your surveillance camera.

**Load balancing** - Load balancing is the distribution of jobs and data throughout the Information Repository. Phoenix RSM queries each Vault regarding the best match for processing requirements, storage resources, free space, and then establishes a connection to the Vault and copies files to the Vault. The network remains load balanced.

**Locator Service** - The Locator Service makes dynamic resource allocation possible which delivers unlimited storage resource accessibility within the network. It works as a virtual middle tier to provide information that enables clients and Vaults to work like a traditional client/server system, but without the need for hard-coded static links between clients and servers. In contrast, the Locator architecture is flexible to allow dynamic client access to any storage resource on your network. The Locator maintains a list of currently available product services, by using a multicast and beacon technology, and it provides this list to clients on the network as needed. To accomplish this, the Locator constantly "listens" for active registered vaults. The Locator list notes Vault status and location changes. Every Locator is self-propagating and shares information with other Locators within the Information Repository.

**Log file** - Error logs are created only when the program encounters a problem. Set the pathname in **Vault Admin** > **Vault Properties** > **logs** to define where error logs are written and stored. An activity log provides logistical information about jobs.

**Log file rotation** - When a new log file is created (error log or activity log), the older file is renamed and the newer log becomes the primary log file. This is log file rotation. You can specify the maximum file size, maximum number of files to keep, and the interval for how often to check if rotation is needed.

**Logging** - The ability to create log entries that are associated with a certain video clip. These log entries contain information about a clip such as time in and time out, the user who created it, date and time created, bullet color associated with the clip, and the title and description of the clip

**Low-resolution companion/proxy file** - Playable video, a fraction of the size of the original video, created when video is captured. This primary video footage remains online and is always teamed with the original source video, even if original is stored near-line or offline. This allows for quick and easy search and play back of video, or seamless video export video to a desktop.

**M**

**Media** - Recording media is a device used to store data or information. Examples of media are hard disk, optical disc, and data tapes.

**Megapixel (HD)** - A megapixel is one million pixels; representing the number of pixels in an image, or the number of elements in a digital display. HD is a type of megapixel camera.

**Metadata** - Data describing digital content.

**Migrate** - The process of moving video and files from one storage area to another. This process is managed by the Data Services Service.

© 2015

**N**

**NAS** - Network Attached Storage. Networked computer that provides file-based data storage.

**Network Activity** - Application used to monitor all data, media, and Vault operations within the Information Repository in real-time.

**NVR** - Network Video Recorder records video in a digital format over a network. The video is encoded and processed at the camera and then streamed into the NVR for storage or viewing. The video is of good quality, with high megapixel resolution.

**O**

**On-Media Catalog** - The metadata catalog, stored on every media unit, that contains metadata for all the files. The on-media catalog is an Information Repository safeguard. Should a Vault catalog become lost or corrupted, the on-media catalogs are used to rebuild it.

**P**

**Patrols** - A group of layouts, where each layout in a patrol is displayed in the Live Viewer for a set amount of time before the next layout is displayed.

**Physical Media** - A physical unit of media, such as a tape, that is independent of its drive. An individual unit of physical media can be used in a single stand-alone drive, or can be one of several units of media within an automated library system. In automated libraries, storage units use robotics to move units of media. With systems based on physical media, there can be one or more drives and several units of media per drive.

**POE** - Power Over Ethernet is a technology used to power network-connected devices through the network.

**Policies** - Phoenix RSM employs the use of "policies". They are the method outlined by parameters and options for managing all your digital assets effectively. In Camera policies, recording policies control from which cameras videos are being captured and when. In Data Service policies, policies control when files are moved, copied, and purged in the Information Repository.

**PTZ** - Pan-Tilt-Zoom is a term used to refer to cameras which have the ability to change their view remotely through a viewer.

**Purge** - The process of deleting video and files from the storage. This process is managed by the Data Services Service.

**Q**

**R**

**Replicate** - The process of copying video and files from one storage area to another. This process is managed by the Data Services Service.

**Resolution** - Resolution refers to the horizontal and vertical size of video in pixels. The larger the frame size, the larger the picture or video in pixels. Higher resolution is normally equated to better quality video.

**RTSP** - Real-Time Streaming Protocol (RTSP) is a network control protocol to control streaming media servers for establishing media sessions between end points. This product is compatible with over 1,000 camera models from over 170 network camera manufacturers.

*© 2015*

**S**

**Server -** Unlike servers that require dedicated computers, product servers can run on any of the computers on your network. The server is composed of various components that manage several operations: registration of location with service modules, responding to client queries about resource availability, negotiating connections with client components, receiving data from clients and storing it properly, receiving metadata from clients and updating the Vault, receiving CRC data from clients and using it for media write validation, informing clients of success and failure during processing, informing client components of matches and mismatches of the CRC, on-media data formatting, receiving data lookup requests from clients, locating restore data within the Vault, responding to client requests for data retrieval, and supplying data to clients as required. During installation, the "Server" version refers to the full suite of Phoenix RSM applications, including Vaults. In contrast, the "Client" version does not include Vaults.

**Service** - A process that runs in the background and performs a specific operation at predefined times or in response to certain events.

**Source** - Refers to the location where data is captured, ingested, or extracted.

**Static IP** - A network address which does not change. Normally used to refer to the process of manually setting the IP address of network devices.

**Storage Pool** - One or more pieces of media grouped for a common use. Additional media can be added to storage pools at any time, and searches can be limited to single storage pools with countless units of media, regardless of which Vaults the media resides on.

**stx** - A file that includes all the video dialog and dialog time codes associated in the video. The .stx file is necessary for searching content in videos, and the name of it matches the video file name.

**Surveillance Video Manager** - Application to search, review, and export video (and metadata) managed in the Information Repository to any computer on the network.

**T**

**Thumbnail** - A thumbnail is a picture or snap shot in time of a video. Thumbnails are used to help the user get a glimpse of activity in video at specified intervals.

**U**

**URL** - Stands for Uniform Resource Locator. A URL is a resource identifier that specifies where an identified resource is available. URLs of RTSP-enabled IP cameras are used to connect them to Phoenix RSM.

**V**

**Vault** - A Vault is comprised of a central processing unit (CPU), Phoenix RSM (software), and storage. Each Vault requires its own capacity license because of its scalable possibilities. The Vaults on the network make up the Information Repository to manage all your data storage needs. The Vaults have attributes associated to them like licensing, media, and files, and are easy to upgrade. They are decentralized, making the Information Repository a distributed solution across your network.

**Vault Admin** - Optional desktop client application used to prepare media and manage media in the Information Repository Vaults.

**Vault Service** - The Vault service manages the video and storage devices.

*© 2015*

**Video Lifecycle Management (VLM)** - A video aware subset of Information Lifecycle Management, providing a comprehensive approach to managing captured video and its associated metadata.

**Virtual Media** - Space set aside for use by a Vault on a storage device also used for other purposes. A hard disk is an example of virtual media. Media units on a hard disk are actually file system directories set up by the Vault. Mapping a Vault to an entire hard disk, Virtual hard disk media units enable you to remove removable disks from Vaults just as you would physical media (such as tapes). Virtual media units can span multiple disk drives or be set so that several virtual media units reside on a single disk drive.

**W**

**Watermark** - Marking video with embedded information to serve as visible identification.

**X**

**Y**

**Z**

2015, 6.5

© 2015

# Index


## - A -

Add a Camera 149, 209
Add a Vault 56
Architecture 16

## - C -

Camera 148
  Add Camera 149, 218
  Motion Detection 226
  Wizard 149
Camera Configurations 198, 200
Camera Policies 158
  Create a Policy 159
  Delete a Policy 159, 161, 162
  Modify a Policy 159, 161
  Window 177
Camera Pools 239
Camera Ports 235
Command Line Arguments 399, 401, 413, 424
Companion Video File 251
Content Searching 338
Customize 331

## - D -

Data Service Policies 297
  Create a Policy 297
  Delete a Policy 297, 298, 300
  Modify a Policy 297, 298
  Window 311
Data Services Service 423
Directory Filters 343

## - E -

Export 162, 203, 300
Export Extensions 349
Export Queue 253

## - F -

FAQs 428
File Filters 343
Firewall 22
Focus 244

## - H -

Histogram 269

## - I -

Import 162, 203, 300
Information Repository 17
Installation 21
  Linux 36
  Macintosh 32
  Windows 24

## - J -

Job Scheduling 192, 322, 425

## - K -

Key Configurations 370

## - L -

License
  Add 95
  Product Licensing 15
Live Viewer 235
  Camera Control 244
  Control Panels 238
  Layout 240
  Patrols 242
  User Preferences 247
  View Camera Feeds 239
Locator Service 400
Log Files 103, 438


© 2015

## - M -

Media 110
Erase 128
Load 120
Reload 123
Unload 124
Migrate 297
Monitor Jobs 135
Motion Detection 226
Multicast 23, 380
Multi-tiered 5

## - P -

Patrols 242
Prepare Media 110
Problems 428
PTZ 244
Purge 297

## - R -

Recording 159
Replicate 297
Rimage 292
RTSP Enabled IP Camera 148, 209, 235

## - S -

Scalable 5
SCSI 77
Search 257
Search Criteria 253
Search Results 253
Status 129, 135
Storyboard 270
Surveillance Video Manager 251
Export Video 277
Media Viewer 265
Search Video 257
User Preferences 288
SVM 251
System Requirements 12

## - T -

Technical Information 18
Terms 441
Troubleshooting 428

## - U -

User Preferences 197, 247, 288

## - V -

Vault 53
Add Vault 54
Checkup 109
Details 129
License 95
Remove Vault 145
Security 85, 99
Shutdown 86
Start Manually 129
Stats 138, 140
Wizard 56
Vault Admin 80
Vault Properties 86
Vault Service 405
Video Feeds 235
VMS 148, 218

## - W -

Watermark 278, 319
Wildcards 332
Wizard 56, 149

© 2015